بسم الله الرحمن الرحيم

تجنب النقطة العمياء في الشبكات اللاسلكية الآنية

Black Hole Avoidance in Ad Hoc Networks

إعداد
زاهي محمود احمد يعقوب
٠٤٢٠٩٠١٠٠٥

المشرف

الدكتور أكرم حمارشه

المشرف المشارك

الدكتور إسماعيل عبابنة

أعضاء لجنة المناقشة	التوقيع
د. أكرم حمارشه	…………………
د. إسماعيل عبابنة	…………………
ا. د عدنان الصمادي	…………………
د. احمد الدلالعة	…………………
د. سعد بني محمد	…………………

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في علوم الحاسوب في كلية /معهد الأمير الحسين بن عبد الله لتكنولوجيا المعلومات في جامعة آل البيت .

نوقشت وأوصي بإجازتها بتاريخ: / / ٢٠٠٩

الإهداء

إلى رفيقة دربي زوجتي العزيزة.

إلى أبنائي الأعزاء.

إلى كل جندي مجهول في هذا الوطن الغالي

أهدي هذا العمل

شكر

أتوجه بالشكر الجزيل إلى مشرفيً وأساتذتي الكريمين الدكتور أكـــرم حمارشـــه والـــدكتور إسماعيل عبابنه اللذين ما بخلا علي بوقتهما ونصائحهما والتي لولاها لما استطعت أن أتم هذا العمل سائلا المولى عز وجل أن يجزيهما عني خير الجزاء، والشكر موصول إلـــى أعـــضاء لجنة المناقشة لتفضلهم بمناقشة هذه الرسالة.

كما أتوجه بشكر خاص إلى الزميل والصديق العزيز بلال كراسنه الذي كان خير معين لي في رسالتي سائلاً المولى عز وجل أن يجزيه عني خير الجزاء.

المحتويات

الموضوع **الصفحة**

الفصل الثاني: أنواع وأشكال الاعتداءات التي تتعرض لها الشبكات اللاسلكية الآنية

الفصل الثالث: مشكلة النقطة العمياء(Black hole) في الشبكات اللاسلكية الانية

الفصل الرابع: الدراسة المقترحة لمواجهة مشكلة النقطة العمياء

الفصل الخامس: المحاكاة

الملحق(أ)

المحاكي المستخدم

قائمة الأشكال

قائمة الجداول

قائمة المصطلحات

AODV	Ad hoc On Demand Distance Vector Protocol	بروتوكول متجه المسافة حسب الطلب الآني
BH	Black Hole	نقطة عمياء
CTS	Clear To Send	جاهزة للاستلام
DSR	Dynamic Source Routing Protocol	بروتوكول المصدري الديناميكي
OSI	Open System Information Interchange	نظام الاتصال المفتوح
PDA	Personal Digital Assistant	المساعدات الشخصية الرقمية
RERR	Rout Error	رسالة خطا مسار
RREP	Route Reply	رسالة رد مسار
RREQ	Route Request	طلب مسار
RTS	Request To Send	طلب إرسال
TCP/IP	Transmission Protocol/ Internet Protocol	بروتوكول
ZRP	Zone Routing Protocol	بروتوكول منطقة التمرير

الملخص

إلا أن هذا النوع من الشبكات، يعاني الكثير من نقاط الضعف، والتي تجعل منها هدفا سهلا للاعتداءات بكافة أشكالها، ويعود سبب ذلك لعدم اللامركزية فيها، ولاستخدامها القنوات اللاسلكية في التراسل والتواصل بين عقدها، مما يسهل عمليات التصنت والاختراق على أعدائها. وقد تناولنا في هذه الدراسة أهم مزايا وخصائص الشبكات اللاسلكية الآنية، ونقاط الضعف فيها. وكذلك أنواع وأشكال الاعتداءات التي يمكن أن تتعرض لها، ومن أشكال تلك الاعتداءات مشكلة النقطة العمياء، وهي من المشاكل الخطيرة ال

تحدث مشكلة النقطة العمياء عندما تقوم احد العقد الغريبة بالدخول إلى الشبكة والاستحواذ على مسار البيانات بين المرسل والمستقبل ومن ثم تقوم بحذف جميع حزم البيانات المارة بها مما يمنع وصولها إلى وجهتها. ويعتمد مقدار الضرر الذي تسببه تلك المشكلة على موقع العقدة الغريبة في الشبكة، وعدد العقد الغريبة التي تمارس هذا الدور.

قدمنا هذه الدراسة آلية لإبعاد اثر مشكلة النقطة العمياء في البروتوكول متجه المسافة حين الطلب الآني (AODV) من خلال تعديل هذا البروتوكول، وتمت مقارنته مع البروتوكول الأصلي بعد إضافة عقدة غريبة علية ثم عقدتين. استخدمنا المحاكي (GloMoSim) لتنفيذ عملية المقارنة حيث أشارت النتائج إلى تحسين أداء البروتوكول، حيث زاد معدل نسب تسليم الحزم إلى ٦٣% وزاد معدل الإنتاجية ٨٠% ومعدل الحزم المسقطة نقص بنسبة ٤٨%.

الفصل الأول

المقـدمـــــة

١-١ تقديم

ُيمكن تعريف الشبكات اللاسلكية الآنية المتحركة (Mobile Wireless Ad Hoc Networks) بأنها مجموعة من العقد اللاسلكية المتحركة التي تتعاون من اجل تامين الاتصال والتراسل فيما بينها، فكل عقدة فـي الـشبكة قـد تكـون مرسـلا (Sender) أو مـستقبلا (Receiver) أو وسـيطا (Intermediate) تؤمن الاتصال للعقد الأخرى، وهذه الشبكات لا تمتلك أي محطات ثابتة (Base Stations) أو أي مركز للمراقبة والسيطرة أو أي بناً تحتية أخرى، وتعتبر مـن أكثـر أنـواع الشبكات عرضة للاعتداءات والتهديدات التي تواجه الشبكات الحاسوبية بشكل عام، والـشبكات اللاسلكية بشكل خاص، ويعود ذلك إلى خصائص هذه الشبكات من جهة والى مجال استخداماتها من جهة أخرى، خاصة إذا استخدمت في العمليات العسكرية وبعض المجالات الحساسة الأخرى (Kong et al, ٢٠٠٥).

١-٢ خصائص ومميزات الشبكات اللاسلكية الآنية

تمتاز الشبكات اللاسلكية الآنية (MANETs) عن غيرها من الشبكات بمجموعة من الخـصائص والمزايا نلخصها في النقاط الآتية (Mir and Wani, ٢٠٠٣)، (Mukherjee et. al, ٢٠٠٣) :

١- عدم امتلاكها لأي بنية تحتية (Infrastructure) ثابتة، فهي مكونة من مجموعة مـن العقـد التي تتعاون فيما بينها لتامين عملية التراسل، فقد تكون العقـدة مـصدراً (Source) أو وجهـة (Destination) أو محولا (Router) يقوم بتمرير الرسائل للعقد الأخرى، ولهذا يصعب مراقبـة العقد ومراقبة أداءها.

٢- ديناميكية الشكل (Topology) وذلك نتيجة لحركة العقد الدائمة، مما يسبب الانقطاع الدائم في المسارات بين العقد وخروج بعض العقد من الشبكة ودخول أخرى، وهذا أيضا يجعـل تحديـد مواقع العقد أمرا صعباً وبالتالي يصعب مراقبة أداءها وسلوكها.

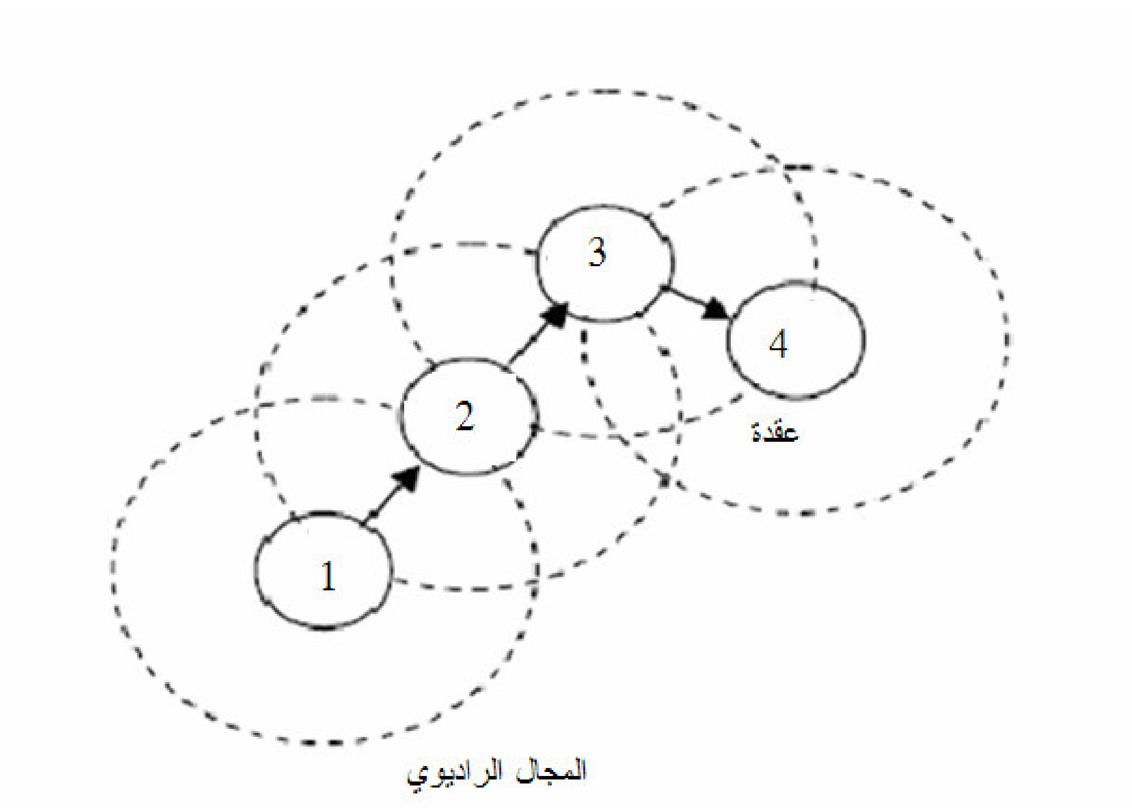
٣- اللامركزية، فلا توجد عقدة مركزية بالشبكة للتعرف على هوية العقد وتحديد صـلاحياتها ومراقبة أداءها أو إصدار تصريح لدخول الشبكة لأي عقدة ترغب في هذا الدخول، فكل العقـد متكافئة في الصلاحيات والمسؤوليات وتستخدم نفس البروتوكولات بكل طبقاتها.

٤- محدودية موارد العقد، فالعقد إما أن تكون أجهزة حواسيب محمولة (Laptops) أو اصـــغر من ذلك وهي ما يسمى بالمساعدات الشخصية الرقمية (Personal Digital Assistants- PDAs) ويشمل ذلك مصدر الطاقة حيث تزود الأجهزة ببطاريات خاصة محدودة القدرة تمكنها من العمل لساعات قليلة فقط، وكذلك سعة الذاكرة وسرعة وقدرة المعالجة لوحدات المعالجة فيهـــا تكـــون محدودة.

٥- سهولة نشرها وتشكيلها فهي ذاتية البناء والإعداد.

٦- تستخدم قنوات الاتصال اللاسلكي المفتوحة في التراسل ونقل البيانات، وهـــذا النـــوع مـــن قنوات الاتصال يسُهل الدخول إليها من أي عقدة تريد ذلك سواءً كانت عقده شرعية تنتمي لنفس الشبكة أو أي عقدة غريبة عنها.

يبين الشكل (١-١) نموذج شبكة لاسلكية أنية مكونة من أربعة عقد والمجال الراديوي لكل عقدة، وتبين الأسهم آلية التراسل بين العقدة (١) والعقدة (٤) من خلال العقد (٢ و٣).



الشكل (١-١) شبكة لاسلكية آنية مكونة من أربع عقد.

١-٣ مجالات استخدام الشبكات اللاسلكية الآنية

نلاحظ مما سبق من مزايا وخصائص هذه الشبكات أنها تلاءم مجموعة من المجالات والظروف ولا يمكن لغيرها من الشبكات أن تعمل في نفس ظروفها، واهم المجالات المعنية هي (Gavini, ٢٠٠٤):

١- حالات الطوارئ الناتجة عن الكوارث الطبيعية كالزلازل والفيضانات والتي عادة ما تتعطل فيها البنى التحتية للاتصالات سواء كانت سلكية أو لاسلكية ذات محطات ثابتة أو حتى مصادر الطاقة التي تغذيها.

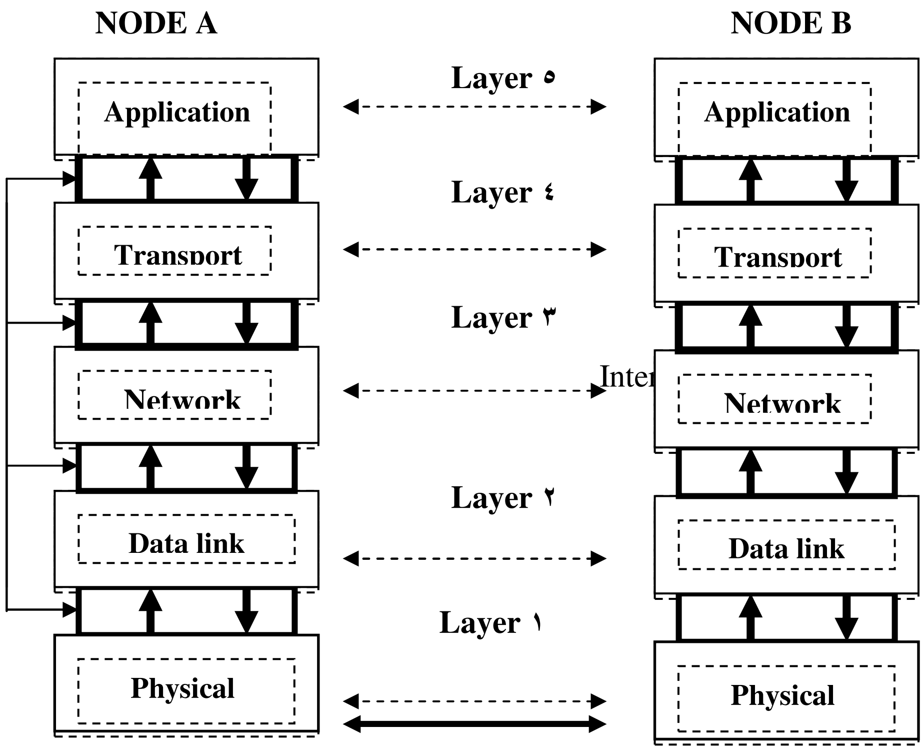
٢- المجالات العسكرية والعمليات الحربية والتي لا يمكن إنشاء بناً تحتية للاتصالات فيها نظراً لحركتها الدائمة وتغير مواقعها كما هو الحال في البحار والمحيطات، وقد تكون أهدافا سهلة للعدو في حال توفر تلك البنى.

٣- في مجال الرحلات الاستكشافية والعلمية والتي تقوم بها مجموعات وفرق من الهواة أو المتخصصين في مجال علوم الطبيعة أو الآثار وما شابه ذلك لبعد المناطق التي يعملون فيها عن المناطق الحضرية ولمدة زمنية محدودة.

٤- في مجال المؤتمرات والندوات حيث توفر التواصل بين المؤتمرين بشكل هادئ لا يوثر على سير أعمال تلك المؤتمرات.

١-٤ البروتوكولات التي تدعم عمل الشبكات الآنية

لقد تم تقسيم بروتوكولات الشبكات الآنية إلى خمس طبقات على غرار نظام (OSI) ذو السبع طبقات ونظام (TCP/IP)، وذلك لتسهيل عمليات الإضافة والتعديل والتطوير لها، وكل طبقة تتكون من مجموعة من البروتوكولات المنفصلة عن بعضها مما يمكن المطورون من إجراء التعديلات عليها أو إضافة بروتوكولات أخرى. وكل طبقة منها تخدم الطبقة التي تعلوها عن طريق واجهة (Interface) تربط بينهما وبالعكس، وذلك كما هو مُبين في الشكل (١-٢)، وما يهم في هذا البحث هو التعرف على بروتوكولات التمرير أو طبقة الشبكة (Network Layer) وهي المستهدفة في هذه الدراسة بغرض تحسين أمنها بمواجهة الاعتداءات المحتملة عليها.



الشكل (١-٢) طبقات بروتوكولات الشبكات الآنية.

١-٤-١ بروتوكولات التمرير (Routing Protocols)

تقسم بروتوكولات التمرير إلى ثلاثة أنواع هي:

١-٤-١-١ البروتوكولات الموجهة بالجداول (Table- Driven Protocols) .

هي بروتوكولات تستخدم الجداول في تخزين المسارات في العقد، ويتم تبادل رسائل التحديث بينها بشكل مستمر لمعرفة التغيرات التي تتم على هيكلية الشبكة، إذ تتعرف العقد على العقد المجاورة لها وتستخدمها لتمرير حزم البيانات عند ورودها، فكل عقدة في الشبكة تعرف باستمرار العقد المجاورة لها (العقد التي تقع ضمن المجال الراديوي لها)، وهذا يسرع عملية نقل حزم البيانات، إلا أن التحديث المستمر من الجيران يعني زيادة عدد حزم التحكم مما يزيد من الكلفة الإضافية.

ومن الأمثلة على هذا النوع من البروتوكولات بروتوكول متجه المسافة المتسلسل (Destination Sequenced Distance Vector - DSDV)، وبروتوكول التمرير اللاسلكي (Wireless Routing Protocol - WRP).

١-٤-١-٢ البروتوكولات الموجهة حسب طلب المصدر

(Source-Initiated On-Demand Routing Protocols)

هي البروتوكولات التي يتم فيها تحديد المسارات عند طلب المرسل، وما يميز هذه البروتوكولات عن غيرها أنها تقوم بتحديد وإنشاء مسارات التمرير فقط عند الحاجة إليها، وبالتالي تقل الكلفة الإضافية مقارنة بالكلفة الإضافية الناتجة عن الرسائل الدورية التي تستخدمها بروتوكولات النوع الأول.

ومن أشهر البروتوكولات من هذا النوع البروتوكول المصدري الديناميكي (DSR) (Johnson and Maltz, ١٩٩٦)، وبروتوكول متجه المسافة حسب الطلب الآني (AODV) (Perkins and Royer, ٢٠٠١)

أ – **البروتوكول المصدري الديناميكي** (DSR): يعتبر هذا البروتوكول من أشهر بروتوكولات التمرير في الشبكات اللاسلكية الآنية بشكل عام، وعملية توجيه الحزم تتم من قبل العقدة المصدر، حيث تضع المسار في رأس حزمة البيانات وترسلها للعقدة الأولى التي تليها في المسار (Johnson and Maltz, ١٩٩٦).

تقوم آلية عمل هذا البروتوكول على آليتين هما: اكتشاف أو طلب مسار من قبل العقدة التي تريد إرسال حزم بيانات، وصيانة المسارات عند انقطاعها نتيجة لحركة العقد.

عندما تريد عقدة إرسال حزم بيانات إلى عقدة أخرى تقوم بالبحث في المسارات المخزنة في ذاكرتها عن مسار إلى تلك العقدة، فإذا وجدت واحداً تقوم بنسخه إلى رأس حزم البيانات ثم تقوم بالإرسال، وإذا لم تجد مساراً، ترسل رسالة طلب مسار إلي جميع العقد في الشبكة (RREQ) وتضع فيها عنوانها وعنوان العقدة المطلوبة وعداداً لقياس عدد القفزات ورقم الطلب (Johnson and Maltz, ١٩٩٦).

تقوم كل عقدة تستلم رسالة الطلب بمعالجة، فإذا كانت هي العقدة المطلوبة تقوم بإرسال رسالة رد (RREP) تضع فيه عداد القفزات بعد أن تضيف إليه العدد واحد وعنوانها وترسله إلى العقدة المصدر والتي تقوم بدورها بتخزينه في ذاكرتها، أما إذا لم تكن هي المستهدفة تقوم بالبحث في ذاكرتها عن مسار إلى العقدة المطلوبة، فإذا وجدت مسارا تقوم بنسخه إلى رسالة الرد، وتضيف إلى عداد القفزات طول ذلك المسار وتقوم بالرد على رسالة الطلب، وإذا لم

تجد مسارا فإنها تقوم بإضافة عنوانها إلى رسالة الطلب وتضيف العدد واحد إلى عداد القفزات فيها وتعيد بث رسالة الطلب مرة أخرى. وإذا تكررت رسالة الطلب نفسها تقوم العقدة بإهمال الطلب وحذف الرسالة (Johnson and Maltz, ١٩٩٦).

أما آلية صيانة المسارات فتبدأ عند حصول انقطاع في احد المسارات، وذلك عندما يتعذر على عقدة وسيطة تمرير حزم البيانات إلى العقدة التي تليها نتيجة لحركة العقد المستمرة وتغيير مواقعها، فتقوم بحذف المسار من ذاكرتها وإرسال رسالة خطأ إلى العقدة المصدر والتي تقوم بمعالجة رسالة الخطأ بحذف ذلك المسار الذي حدث فيه الانقطاع، والبحث عن مسار بديل في ذاكرتها، وان لم تجد تبحث عن مسار جديد (Johnson and Maltz, ١٩٩٦).

وقد تم تعديل هذا البروتوكول ولعدة مرات من اجل زيادة كفاءته وتقليل عدد المسارات المخزنة في ذواكر العقد وتقليل عدد حزم التحكم، وكذلك إنقاذ حزم البيانات عند انقطاع المسار وغيرها من التعديلات (عبد الله، ٢٠٠٦).

ب- بروتوكول متجه المسافة حسب الطلب للشبكات اللاسلكية الآنية

Ad Hoc on-Demand Distance Vector (AODV)

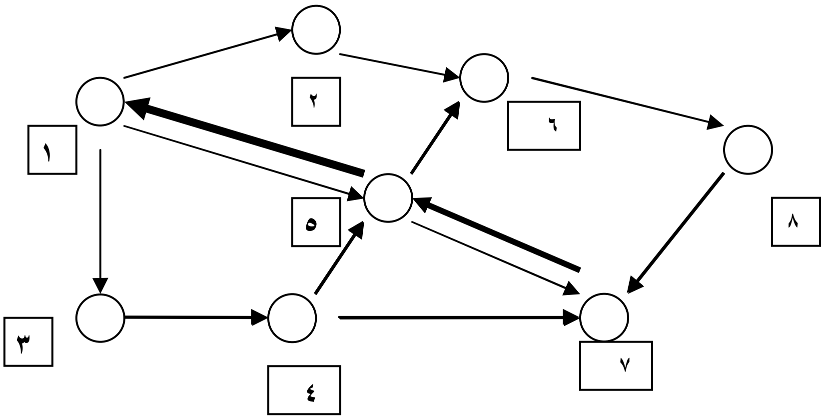
هذا البروتوكول من البروتوكولات الموجهة حسب طلب المصدر، ويحوي هذا البروتوكول على آليتين هما آلية اكتشاف المسار (Route Discovery) وآلية إدامة المسار (Route Maintenance).

آلية اكتشاف المسار

عندما تريد عقدة أن ترسل حزمة معطيات لهدف ما فإنها تبحث أولا في جدول مساراتها (Routes Table) عن مسار غير منتهي الصلاحية (Active)، فإذا وجدت فإن حزمة البيانات ترسل إلى المحطة التالية (Next Hop) في هذا المسار، وهي بدورها ترسلها إلى العقدة التي بعدها في المسار، وهكذا دواليك حتى الوصول للهدف، أما إذا لم يتم العثور على مسار فيتم استدعاء آلية اكتشاف المسار عن طريق إرسال رسالة طلب مسار (Route Request) تحوي عنوان المصدر وعنوان الهدف ورقماً متسلسلاً للهدف (Sequence Number) ورقماً متسلسلاً للبث (Broadcast Number) تتم زيادته في كل مرة يتم فيها تهيئة رسالة طلب مسار جديد. يتم بث رسالة طلب المسار إلى جيران المصدر فإذا لم يكن أحدهم الهدف أو لم يكن لديه مسار للهدف فإنه ينشر الطلب بدوره إلى جيرانه، وهكذا حتى الوصول إلى الهدف أو إلى عقدة لديها مسار للهدف (Perkins and Royer, ٢٠٠١). أية عقدة تستقبل رسالة طلب مسار تتأكد من أنها

لم تستلم هذا الطلب من قبل – وإذا كانت قد استلمته فإنها تحذفه – فإذا لم تكن قد استلمته فإنها تنشئ له مدخلاً (Entry) في جدول خاص بتخزين رسائل الطلب، ويحوي هذا المدخل عنوان المصدر ورقم البث، وإذا كانت العقدة هي الهدف أو تملك مساراً للهدف فإنها ترسل رسالة جواب مسار (RREP) إلى المصدر. يحوي الجواب أحدث رقم متسلسل للهدف وعدد القفزات (Hops) حتى الهدف وفترة صلاحية هذا المسار (Perkins and Royer, ٢٠٠١).

خلال عبور رسالة طلب المسار للعقد الوسيطة باتجاه الهدف يتم إنشاء مدخل يدعى مدخل المسار العكسي (Reverse Path Entry) في جدول المسارات لهذه العقد. يحوي هذا المدخل المحطة التالية باتجاه المصدر وعنوان المصدر والرقم المتسلسل للهدف وعدد المحطات حتى المصدر، ويتم كذلك خلال مرور رسالة الجواب عبر العقد الوسيطة باتجاه المصدر إنشاء مدخل يدعى مدخل المسار الأمامي (Forward Path Entry) في جدول المسارات لهذه العقد أيضاً، يحوي هذا المدخل المحطة التالية باتجاه الهدف وعنوان المصدر وعدد القفزات حتى الهدف.



الشكل (١–٣) آلية طلب المسار والرد في البرتوكول (AODV).

في الشكل (١–٣) العقدة (١) تطلب مسارا إلى العقدة (٧) لعدم وجود مسار إليها في جدول المسارات. تبث العقدة (١) رسالة طلب مسار تصل العقد المجاورة لها وهي العقد (٢، ٥، ٣).

تقوم العقد (٢، ٥ ،٣) بالبحث عن مسار مفعل في جداول المسارات لديها يوصل إلى العقدة (٧)

فان وجدت تقوم بإرسال رسالة رد إلى العقدة (١) تخبرها بوجود مسار إلى العقدة (٧)، وإلا فإنها تقوم ببث رسالة طلب أخرى إلى العقد ألمجاوره لها، حيث تقوم العقد (٤،٦) بمعالجة الطلب وبنفس الآلية، إلى أن تنتهي عملية الطلب برسالة رد بوجود مسار إلى العقدة الهدف (٧). يتم اختيار المسار (١–٥–٧) لإرسال حزم البيانات وذلك لكونه اقل المسارات في عدد القفزات.

آلية إدامة المسار

تقوم هذه الآلية بالحفاظ على المسار ما دام المصدر يحتاجه، فإذا تحركت العقدة المصدر أثناء البحث عن مسار لحزمة معطياتها يعاد استدعاء آلية اكتشاف المسار، أما إذا تحركت العقدة الهدف أو أي عقدة وسيطة ضمن المسار تقوم العقدة التي حدث عندها الخطأ بإرسال رسالة خطأ مسار (Route Error Message) إلى كل المصادر المتأثرة التي يمكن أن تستخدم هذا المسار (Perkins and Royer, ٢٠٠١).

وهناك آليتان لاكتشاف الخطأ في المسار الأولي وتحديث جدول المسارات، الأولى تستخدم بروتوكول نقل البيانات (MAC ٨٠٢. ١١)، ويتم في هذا البروتوكول بث رسالة طلب إرسال من العقدة المرسلة إلى العقدة المستلمة (RTS) وعند استلام هذه الرسالة تقوم العقدة المستلمة بالرد عليها برسالة إشعار بأنها جاهزة للاستلام (CTS) ويتم إرسال حزم البيانات، وتنتظر العقدة المرسلة إشعار تسلم (Acknowledgment) من العقدة المستلمة، وإذا لم يصلها إشعار بذلك تقوم العقدة المرسلة بإعادة الإرسال لعدد محدود من المرات، وإذا لم تنجح في الإرسال تقوم بتمرير رسالة خطا إلى طبقة الشبكة (Network Layer) والتي بدورها تقوم بمعالجة الرسالة وإرسال رسالة خطا (RERR) إلى العقدة المصدر، ويتم تحديث جدول المسارات بحذف المسار الذي حصل فيه الانقطاع.

أما الإلية الأخرى فتتم في طبقة الشبكة نفسها حيت تقوم العقد ببث رسائل تعريف (Hello Messages) للعقد المجاورة لها وبشكل متبادل، فكل عقدة تسمع هذه الرسائل تقوم بتحديث المسار الذي تقع عليه العقدة المرسلة بزيادة فترة صلاحيته وإلا فيعتبر ذلك المسار غير مفعل ولا يتم تحديثه إلا إذا تم استخدامه مرة أخرى (Perkins et al, ٢٠٠٣).

١-٤-١-٣ **البروتوكولات المهجنة** (Hybrid Protocols)

هي البروتوكولات التي تجمع بين البروتوكولات الموجهة بالجداول والبروتوكولات الموجهة حسب طلب المصدر، حيث تقسم الشبكة إلى عدة مناطق تمرير. تتشكل منطقة التمرير لعقدة ما من العقد التي تبعد عن هذه العقدة عدة قفزات، وتستخدم البروتوكولات الموجهة بالجداول داخل مناطق التمرير، بينما تستخدم البروتوكولات الموجهة حسب طلب المصدر للتمرير بين مناطق التمرير. ومن هذا النوع من البروتوكولات سنذكر وبشيء من الاختصار بروتوكول منطقة التمرير (Zone Routing Protocol –ZRP) (Mukherjee et al, ٢٠٠٣) .

أ- بروتوكول منطقة التمرير

تنتمي كل عقدة في هذا البروتوكول إلى منطقة تمرير، حيث يتم بناء منطقة التمرير نسبة إلى عدد العقد، فمثلاً نقول أن العقدة أ وجيرانها على بعد لا يتجاوز خمس عقد تشكل منطقة تمرير. كل عقدة يجب أن تعرف هيكلية منطقة تمريرها فقط، وتنشر التعديلات التي تطرأ على الشبكة داخل كل منطقة تمرير. تستخدم البروتوكولات الموجهة بالجداول مثل بروتوكول متجه المسافة حسب الوجهة داخل مناطق التمرير، أما خارج مناطق التمرير فتستخدم البروتوكولات الموجهة حسب طلب المصدر مثل بروتوكول متجه المسافة حسب الطلب الآني. يتميز بروتوكول منطقة التمرير بتخفيف الكلفة الإضافية مقارنة مع البروتوكولات الموجهة بالجداول وباكتشاف المسار بشكل أسرع مقارنة مع البروتوكولات الموجهة حسب طلب المصدر (Mukherjee et al, ٢٠٠٣).

١-٥ دوافع الدراسة

تم في هذه الدراسة معالجة مشكلة مهمة من مشاكل امن الشبكات اللاسلكية الآنية، وهي مشكلة النقطة العمياء. تحدث هذه المشكلة عندما تقوم عقدة غريبة بالدخول إلى الشبكة بعد أن تتجاوز وسائل الأمن والحماية الأولية كإصدار تصريح الدخول، ثم تقوم بعدها بالاستحواذ على مسار البيانات لتبدأ بعدها بحذف كل الحزم التي تمر بها، وبذلك تكون قد عطلت جزءاً من الشبكة أو ربما كلها.

لقد اخترنا في هذه الدراسة البروتوكولات الموجهة حسب طلب المصدر (Source-Initiated On-Demand Routing Protocols)، لكونها من أهم بروتوكولات الشبكات الآنية والتي تعاني من نقاط الضعف في أمنها وسريتها، وقد تم اختيار تطبيق هذه الدراسة على بروتوكول متجه المسافة حسب الطلب للشبكات الآنية (AODV)، حيث لا تعرف العقدة المرسلة كافة العقد الواقعة على المسار إلى الهدف، فهي فقط تعلم عن العقدة التي تليها في المسار، وعدد القفزات إلى الهدف وبالتالي لا يمكن لها معرفة إن كان في المسار عقد غريبة أم لا.

تقع هذه الرسالة في خمس فصول، تم تخصيص هذا الفصل كمقدمة لهذه الدراسة، وأما الفصل الثاني فقد تم فيه عرض نقاط الضعف التي تعاني منها الشبكات الآنية، وأنواع وأشكال الاعتداءات المحتملة عليها، وكذلك متطلبات أنظمة الحماية بشكل عام، والدراسات والمقترحات التي قدمت من اجل حماية الشبكات الآنية واليات وطرق تنفيذ تلك الدراسات.

وأما الفصل الثالث فقد خصص لتوضيح المشكلة التي تمت معالجتها في هذا البحث من حيث كيفية حدوثها، وأثارها على بروتوكولات التمرير، وكذلك الأفكار والمقترحات التي يمكن أن تتبادر إلى ذهن الباحث ومناقشتها، والدراسات التي تناولت موضوع سرية وامن البروتوكولات في الشبكات الآنية بشكل عام.

وأما الفصل الرابع فنتناول فيه الخوارزمية المقترحة لتامين المسارات، وإبعاد اثر العقد الخبيثة التي تسبب حدوث مشكلة النقطة العمياء (Black Hole) في الشبكة وعزلها.

ونتناول في الفصل الخامس تطبيق هذه الخوارزمية على بروتوكول متجه المسافة حسب الطلب (AODV)، ويتم تقييم التعديلات التي قمنا بها على هذا البروتوكول لمعالجة مشكلة النقطة العمياء، وذلك مقارنة بالبروتوكول الأصلي المعدل الذي يحتوي على النقطة العمياء، وكذلك نقوم بعرض وتحليل نتائج .

وفي الفصل السادس نتناول خلاصة هذه الدراسة والدراسات المستقبلية.

ألفصل الثاني

أنواع وأشكال الاعتداءات التي قد تتعرض لها الشبكات اللاسلكية الآنية

٢-١ تقديم

تمتاز الشبكات اللاسلكية الآنية المتنقلة بمرونة عالية في حركة العقد لديها، أضف إلى ذلك سهولة وسرعة تنصيبها وتشغيلها، لذلك فهي تناسب الحالات الطارئة كالكوارث الطبيعة والعمليات الحربية والعسكرية، وكذلك المؤتمرات والمجموعات الاستكشافية، إلا أن هذه الشبكات تعاني من سهولة اختراقها والتنصت عليها من قبل أعداء محتملين خاصة إذا استخدمت في المجال العسكري (Gavini, ٢٠٠٤)، فجميع البروتوكولات المستخدمة في الشبكات اللاسلكية الآنية تعمل بشكل جيد إذا لم تتعرض لأحد أشكال الاعتداءات، وهذا الأمر لا يمكن إهماله أو تجاهله لما له من أثار قد تحبط عمل الشبكة وتهدد أمن البيانات التي تنقلها، وسنذكر هنا أهم نقاط الضعف وأنواع وأشكال التهديدات والاعتداءات المحتملة التي تواجه الشبكات الآنية المتنقلة وكذلك الحلول المقدمة لمواجهة تلك الاعتداءات.

٢-٢ نقاط الضعف التي تعاني منها الشبكات اللاسلكية الآنية:

أ- سهولة سرقة العقد في الشبكة نظراً لسهولة حملها ونقلها وبالتالي يمكن استخدامها مرة أخرى للاعتداء على الشبكة، ويصعب كشفها لكونها عقدة تنتمي للشبكة وتمتلك نفس إمكانيات العقد الأخرى، كبرنامج تشغيل الشبكة وبرتوكولاتها وحتى وسائل الحماية التي قد تزود بها العقد.

ب- محدودية موارد العقد فيها، خاصة البطاريات التي تعتبر المزود الوحيد للطاقة وكذلك سعة الذاكرة، والإمكانات المحدودة لوحدات المعالجة، لكون العقد أجهزة محمولة صغيرة الحجم.

ج- الحركة المستمرة للعقد وما تحدثه هذه الحركة من صعوبة في متابعة العقد ومراقبتها وتحديد مواقعها ومعرفة العقد الداخلة والخارجة من مجال الشبكة.

د- استخدامها قنوات الاتصال اللاسلكية في عملية التراسل بين العقد، وهي قنوات مفتوحة مما يسهل عمليات الاختراق والتنصت (Eavesdropping) والتشويش عليها.

هـ- استخدامها الخوارزميات الموزعة في عملها، خاصة في تعميم ونشر حزم التحكم ضمن المجال الراديوي لها، مما يمكن العقد الغريبة من الاتصال بالشبكة والتواصل مع باقي العقد بيسر وسهولة (Ning and Kun, ٢٠٠٣).

و- بروتوكولاتها التي اعتمد في تصميمها على المقاييس الكمية دون النظر إلى درجة السرية والأمان والوثوقية لتلك المسارات وهذا ينسحب على معظم الدراسات والأبحاث التي قامت بعدها على تحسين تلك البرتوكولات (Yi et al, ٢٠٠١).

٢-٣ أهم المقاييس التي اعتمدت لقياس كفاءة البروتوكولات:

أ- عدد القفزات في المسارات (Hop Account).

ب- عدد المسارات المخزنة في الذواكر (Rout Numbers).

ت- مدة التأخير في استلام الحزم (End- to -End Delay).

ث- عدد الحزم المرسلة في الثانية (Throughput).

ج- عدد الحزم المسقطة أثناء إرسالها (Number of Packets Dropped).

ح- نسبة عدد حزم التحكم إلى عدد حزم البيانات (Overhead).

٢-٤ التهديدات والاعتداءات المحتملة في الشبكات اللاسلكية الآنية.

(Attacks and Threats in Ad hoc Networks).

يمكن تصنيف الاعتداءات التي تواجه الشبكات اللاسلكية الآنية بشكل خاص على أسس مختلفة، فمن ناحية تأثيرها على عمل الشبكة تصنف إلى صنفين هما:

أولا: الاعتداءات التي تقوم على التنصت ونسخ البيانات المنقولة عبر الشبكة وهي ما تسمى (Passive Attacks)، وهذا النوع من الاعتداءات يصعب كشفه وذلك لعدم ظهور تأثير مباشر له على الشبكة.

ثانياً: الاعتداءات التي تسبب عطلاً في عمل الشبكة (Active Attacks) كأن تقوم إحدى العقد الغريبة بالاستحواذ على مسار البيانات وتقوم بحذف كل الحزم التي تأتي إليها دون تمريرها إلى

العقدة التي تليها، وهناك أشكال عديدة منها، ويمكن تصنيف هذا النوع بحسب مصدر الاعتـــداء إلى صنفين هما (Anjum and Mouchtaris, ٢٠٠٧):

أ: الاعتداء الداخلي حيث تقوم عقدة من العقد الشرعية في الشبكة بممارسة التخريب فيها كأن ترسل معلومات غير صحيحة عن المسارات أو تحول المسارات إلى غير الوجهة المطلوبة مما ينتج عنه دوران غير منتهي (Loop).

ب: الاعتداء الخارجي، ويكون مصدره عقدة غريبة عن الشبكة، وهذا الصنف يسهل كشفه مقارنة الصنف الأول.

ويمكن التصنيف بحسب الطبقة المستهدفة من الاعتداء إلي الأصناف الآتية:

أولا: الاعتداءات الموجهة لطبقة الشبكة (Network Layer) وبروتوكولات التمرير، ومثـــل تلك الاعتداءات ما يسمى النقطة الدودية (Wormhole) حيث تقوم احد العقد الغريبة باستلام حزم البيانات وتمريرها إلى عقدة غريبة أخرى.

ثانيا : الاعتداءات التي تستهدف طبقة النقل (Transport Layer) حيث تقوم العقـــدة الغريبـــة بالحصول على إذن للدخول إلى الشبكة بعد الحصول على المعلومات والآليـــة اللازمـــة لـــذلك لتظهر وكأنها عقدة شرعية ثم تقوم بأحد أشكال الاعتداءات الأخرى.

ثالثا : اعتداءات طبقة التطبيقات (Application Layer) ومنها البرمجيات الضارة كالفيروسات.

رابعا : اعتداءات متعددة المستويات وهي التي لا يقتصر ضررها على طبقة معينة كان تقـــوم عقده غريبة بالتوسط بين عقدتين شرعيتين ومن ثم التحكم في المسار بينهما وهي ما تسمى ب (Man-in-the-Middle)، وكذلك الحصول على عناوين العقد واستخدامها من اجل عـــزل العقـــد الشرعية في الشبكة.

خامسا : اعتداءات أخرى متفرقة كسرقة الأجهزة المحمولة ونسخ البرامج عنها بغرض تقليـــدها لاستخدامها في الاعتداء مرة أخرى على الشبكة (Liao, ٢٠٠٥).

٢-٥ أشكال الاعتداءات:

أما أشكال الاعتداءات فهي متنوعة بحسب أنواع البروتوكولات وآلية عملها ونقاط الضعف فيها وسنعرض هنا أهمها.

١- التجسس والتنصت (Eavesdropping) حيث تقوم العقد الغريبة بالتنصت على عمليات إرسال حزم البيانات والحصول على نسخ منها بغرض الاستفادة منها.

٢- الاعتراض (Interception) وهو التعرض للموجات اللاسلكية التي تستخدم لنقل الحزم بين العقد في الشبكة.

٣- إغراق الشبكة بحزم التحكم من اجل إحباطها وإضعاف قدرتها، كأن تقوم العقد الغريبة بإرسال طلب مسار (RREQ) وبشكل مستمر لإشغال العقد بمعالجتها مما يحد من كفاءة الشبكة ويقلل من إنتاجيتها ويستنزف مصادر الطاقة المحدودة فيها.

٤- التزوير والتضليل (Forging) عن طريق تغيير محتويات حزم التحكم سواء كانت طلب مسار أو رد وخاصة تغيير معرفات المصدر (Source Identification) أو الهدف (Destination Identification) أو عدد القفزات (Hop Counts) مما يولد عدداً كبيراً من المسارات في جداول المسارات ويستنزف قدرات العقد.

٥- حذف الحزم ومنع وصولها إلى وجهتها خاصة حزم البيانات، وذلك بأن تقوم احد العقد بالاستحواذ على المسار الذي سبق إنشاؤه لتمرير حزم البيانات ومن ثم تقوم بحذف جميع أو بعض حزم البيانات المارة بها، وهذا ما يسمى بمشكلة النقطة العمياء (Black Hole) وهي موضوع هذا البحث.

٢-٦ الأهداف المطلوبة من أنظمة الحماية والسرية في الشبكات اللاسلكية الآنية

يجب على انظمة الامن والحماية بشكل عام ان تسعى الى تحقيق مجموعة من الخدمات والاهداف نذكرها فيما يلي:

١- ان تحقق الخصوصية (Confidentiality) أي أن تراعي خصوصية كل من يتعامل مع الشبكات وتحافظ على سرية البيانات المنقولة عبرها.

٢- ان تحافظ على تكاملية وسلامة البيانات (Integrity) من التدمير او التزوير أو أي شكل من أشكال الإعتداء عليها وفي كل الظروف.

٣- الوثوقية (Authenticity) اي لا تسمح للدخول غير الشرعي إلى الشبكة وتوفر الوسائل الآمنة للدخول المسموح.

٤- التحكم في الوصول إلى موارد الشبكة (Access Control).

٥- تمكين الوصول والعمل في شتى الظروف (Availability).

٢-٧ آليات وخطوات التصدي للعقد الغريبة.

تتلخص خطوات التصدي للعقد الغريبة التي تمارس التخريب في الشبكات الآنيـــة فـــي ثـــلاث مراحل:

أولا: اكتشاف الآثار التي تظهر في الشبكة مثل زيادة عدد حزم التحكم عن المـــألوف وبالتـــالي ضعف الكفاءة.

ثانيا: الكشف والتعرف على العقد التي سببت تلك الآثار السلبية في الشبكة من خلال عناوينهـــا أو مواقعها.

ثالثا: القيام بعزلها من الشبكة وعدم السماح لها بالدخول والتبليغ عنها كعقده غير شرعية.

٢-٨ الدراسات والأبحاث المقدمة لتحسين البروتوكولات لمواجهة الاعتداءات فـــي الـــشبكات الآنية.

يمكن تقسيم الدراسات والأبحاث التي تم تقديمها من أجل سرية وأمن بروتوكـــولات الـــشبكات الآنية بناءً على التحديات والقضايا التي عالجتها:

أولا: التعرف إلى هوية العقدة والتصديق عليها (Authentication) قبل التعامل معها من قبـــل العقد في الشبكة، وذلك من خلال مجموعة من الخوارزميات، وعزلها في حال تبين أنها غريبة عن الشبكة.

ثانيا: استخدام طرق تشفير البيانات أو الحزم (Cryptography) قبل إرســـالها عبـــر مـــسارات الشبكة.

ثالثا: تحسين أمن عملية التمرير في المسارات (Routing Security) وتامين سلامة وصولها إلى وجهتها، وسوف نستعرض بشيء من التفصيل لهذه الدراسات في الفصل الرابع.

٢-٩ امن وسرية الشبكات ذات البنى التحتية

هناك عدة طرق وآليات تستخدم في الشبكات ذات البني التحتية (Infrastructure) للتعرف علـــى العقد التي تدخل إليها ومن خلال معرفات فريدة لهذه العقد، وقد يتطلب ذلك إضافة أجهزه خاصة لهذه الغاية، وبعد التأكد من هوية العقد يصرح لها بالدخول وضمن صلاحيات محددة وتسند هذه العملية إلى جهة خاصة (Certificate Authority-CA) في الشبكة تتولى التحقق من شرعية العقد من خلال معرفاتها (Identifiers).

وهذا أحيانا يتطلب عمليات معالجة كبيرة ومعقدة إذا أضفنا إليهـا عمليـات التـشفير للحـزم المنقولة، لتحقيق الأهداف الأخرى كتحقيق الخصوصية (Confidentiality) وتكامليـة وسـلامة البيانات. وهذا ما يصعب تحقيقه في الشبكات الآنية نظرا لخصائص هذه الشبكات التي ذكـرت آنفا، من محدودية موارد العقد والطاقة والقدرة على المعالجة (Khalili et al, ٢٠٠٣).

الفصل الثالث

مشكلة النقطة العمياء (Black Hole) في الشبكات اللاسلكية الانية

٣-١ تقديم

تعتبر مشكلة حدوث النقطة العمياء من أخطر المشاكل التي تواجه الشبكات اللاسلكية الآنية وذلك لسهولة إحداثها وللضرر الكبير الذي تلحقه في عمل الشبكة، فقد تؤدي إلى تعطيلها كليا أو جزئيا، خاصة إذا قامت أكثر من عقدة غريبة وفي أكثر من موقع بإحداث تلك المشكلة (Awerbuch et al, ٢٠٠٥).

وتختلف آلية حدوث النقطة العمياء بحسب نوع البروتوكولات المستهدفة بهذا النوع من الاعتداءات، وسنتعرض في هذه الدراسة إلي آلية حدوثها في بروتوكولات التمرير حسب الطلب.

٣-٢ كيفية حدوث المشكلة

تحدث هذه المشكلة عندما تقوم عقدة غريبة بالدخول الى الشبكة والتنصت على العقد وعند صدور رسالة طلب من احد العقد في الشبكة تقوم العقدة الغريبة بما يلي:

١- تقوم باستلام رسالة الطلب (RREQ) المرسلة من العقدة المصدر.

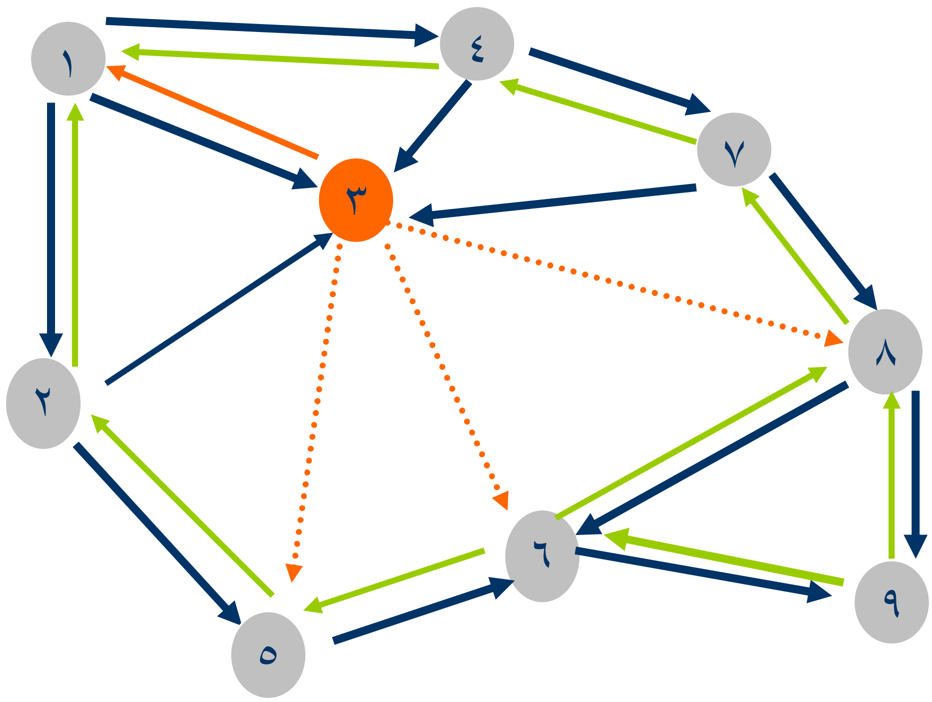
٢- على الفور تقوم بارسال رسالة رد (RREP) مدعية أن لديها مسارا إلى العقدة الهدف، بينما تقوم العقد الأخرى والتي استلمت رسالة طلب مسار في الشبكة بمعالجة الطلب بحسب بروتوكول التمرير المستخدم.

٣- نتيجة للسرعة في الرد غالبا ما تحصل العقد الغريبة على الأولوية بان تكون على المسار الذي سيستخدم في نقل البيانات.

٤- تقوم العقدة المصدر بعد استلامها رسالة الرد (RREP) بارسال البيانات على هذا المسار، وعندها تقوم العقدة الغريبة باستلام البيانات وحذفها على الفور وبالتالي تمنع من وصولها الى الهدف مما يعني تعطل جزء من الشبكة، ويكون حجم الضرر الناتج بحسب موقع العقدة الغريبة في الشبكة، فكلما كانت اقرب على العقدة المصدر كلما كان حجم الضرر أكبر، أما اذا كانت بعيدةً عنها فإن الضرر قد يكون معدوما، وكذلك فان زيادة العقد الغريبة في الشبكة يزيد من احتمالية تعطل الشبكة بالكامل .

والمثال التالي يوضح كيفية حدوث هذه المشكلة.

مثال: في هذا المثال تقوم العقده ١ بطلب مسار الى العقده ٩ ، والعقده ٣ هـي العقـده الغريبة التي تسبب حدوث النقطة العمياء في الشكل (٣-١) على النحو التالي:



الشكل (٣-١) آلية حدوث مشكلة النقطة العمياء.

أ- ترسل العقدة ١ طلب مسارالى العقدة ٩ .

ب- تقوم العقد ٢ و ٣ و ٤ كعقد مجاورة للمصدر باستلام رسالة الطلب.

ج- ترسل العقدة ٣ وعلى الفور رسالة رد الى المصدر مدعية بان لديها مسارا حديثا الى العقدة ٩.

د- تقوم العقد ٢ و٤ بمعالجة رسالة الطلب بالبحث في جدول المسارات لديها عن مسار الى العقدة ٩.

هـ- تقوم هذه العقد بارسال رد الى العقده ١ اذا توفر مثل هذا المسار وإلا تقوم ببث رسالة طلب مسار إلى العقد المجاورة لها (العقد ٥ و ٧) .

و- وهكذا تتكرر الخطوتان الاخيرتان حيث تقوم العقد (٥ و٧) بمعالجة رسالة الطلب حتى بلوغ الهدف.

ز- نتيجة لسرعة العقدة ٣ في الرد على طلب المسار يتم اختيار المسار ١-٣ لإرسال البيانات.

ح- تقوم العقدة ٣ في هذا المثال باحداث مشكلة النقطة العمياء وذلك بحذف حزم البيانات التي تصلها بواسطة الممر ١—٣ وبذلك تعطل عمليات تمرير حزم البيانات، وبالتالي تعطل جزء من الشبكة أو كلها.

نلاحظ أن العقدة التي تسبب هذه المشكلة قد تتجاوز جميع خطوط الدفاع التي استخدمت لحماية بروتوكولات التمرير، فعليها فقط الحصول على تصريح دخول الشبكة ولا تتأثر بعمليات تشفير الحزم وآليات تحقيق التكاملية (Integrity).

٣-٣ الدراسات السابقة المتعلقة بامن عمليات التمرير في الشبكات الانية

إن معظم الدراسات والأبحاث التي تمت مراجعتها انصبت على استخدام آليات وخوارزميات التشفير المتعددة، وعلى استخدام آليات إصدار وتوزيع مفاتيح التشفير بين العقد (Awerbuch et al, ٢٠٠٢)، بغرض التعرف على العقد والسماح لها بدخول الشبكة، وكذلك المحافظة على حزم البيانات من عمليات التنصت والنسخ، وكل هذه الدراسات يمكن وضعها تحت عنوان البروتوكولات الأمينة (Secure Routing) مع أنها تعاني من نقاط ضعف تحت ظروف معينة، كأن تقوم عقدة غريبة بالحصول على مفاتيح التشفير أو أن تقوم بتعطيل ممرات التمرير عن طريق حذف الحزم المشفرة، أو الاحتيال والادعاء بأنها عقدة شرعية عن طريق إسناد أحد معرفات العقد الشرعية لنفسها، ومن الأمثلة على ذلك بروتوكول متجه المسافة حسب الطلب للشبكات الآنية الآمن (Secure Ad Hoc on Demand Vector Protocol-SAODV) وبروتوكول متجه المسافة الآني الآمن (Secure Efficient Ad Hoc Distance Vector Routing-SEAD) والذي تم تطويره عن البروتوكول متجه المسافة المتسلسل (Destination-Sequenced Distance-Vector Routing- DSDV) (Pervaiz et al ٢٠٠٥).

أما في موضوع تحسين أمن عمليات التمرير لبروتوكولات التمرير (Routing Security) فهناك بعض من الأفكار والدراسات في موضوع تجنب النقطة العمياء في الشبكات اللاسلكية الآنية في بروتوكول متجه المسافة عند الطلب (Marti et al, ٢٠٠٠). وهناك دراسات مشابهة تمت على بروتوكول المصدري الديناميكي (DSR).

ومن هذه الأفكار منع العقد الوسيطة في الشبكة من الرد على رسالة طلب المسار، وفي هذه الحالة يتم الرد فقط من قبل العقدة الهدف وبالتالي نضمن مساراً آمنا، إلا أن هذه الفكرة تعاني من بعض الضعف، فمثلا تسبب زيادة في تأخير وصول الرد، وتزيد الكلفة الإضافية المرافقة لطلبات المسار، يمكن أن تقوم العقدة غير الشرعية بالتزوير والإدعاء بأنها العقدة الهدف (Deng et al, ٢٠٠٢).

وقدمت دراسة في هذا المجال اعتمدت آليتين، الأولى تسمى كلب الحراسة (Watchdog) تقوم على مراقبة تصرفات العقد في الشبكة، وتسجل عدد مرات الخطأ التي تقوم بها كل عقدة، ويتم تحديد حد أعلى لذلك إذا تجاوزته أي عقدة يبلغ عنها ويتم عزلها من الشبكة، ويتم دعم هذه الآلية بالآلية الثانية المسماة تحديد معيار المسارات (Path Rater) والتي يتم من خلالها إعطاء كل عقدة في الشبكة قيمة تمثل مدى الثقة بها، ويتم زيادة أو إنقاص تلك القيمة بناءً على تصرفات العقدة، وكل عقدة تطلب مسارا في الشبكة، تزود بهذه القيم لكل عقد المسار، وبناءً عليها يتم حساب قيمة ثقة للمسار، ويتم الاعتماد على هذه القيمة عند اختيار المسار لإرسال حزم البيانات.

وقد تم تطبيق هذه الدراسة على البروتوكول المصدري (Marti et al, ٢٠٠٠).

وهناك دراسة أخرى تحت عنوان منع حدوث النقطة العمياء في الشبكات الآنية المتحركة (Prevention of Blackhole in MANET) تم تطبيقها على بروتوكول متجه المسافة حسب الطلب الآني (Tamilselvan and Sankaranarayanan, ٢٠٠٧) يمكن تلخيصها بالشكل الأتي:

١- تقوم كل عقدة تريد إرسال بيانات بالبحث في جدول المسارات لديها عن مسار يوصلها إلى الهدف وكما هي آلية بروتوكول متجه المسافة حسب الطلب الآني.
٢- إذا لم يتوفر مسار لديها تقوم ببث رسالة طلب مسار إلى العقد المجاورة.
٣- يتم تكرار البند ١ و ٢ في جميع العقد الوسيطة إلى أن يتم اكتشاف مسار إلى الهدف.
٤- عند توفر مسار عند أي عقدة وسيطة يتم إرسال رسالة رد إلى المصدر تتضمن معلومات المسار.
٥- تقوم العقدة المصدر باستلام رسائل الرد من العقد المجاورة لها ويتم إنشاء جدول لتخزين جميع المسارات الواردة ويتم تحديد وقت وصول أول رد.
٦- بعد مرور وقت محدد يتم اختيار مسار من بين المسارات التي يتكرر فيها عنوان العقدة التالية (Next Hop) للعقد المجاورة للمصدر.
٧- في حال عدم توفر مسار بهذه المواصفة، يتم اختيار مسار بشكل عشوائي ويتم إرسال البيانات مباشرة.

استخدم الباحث المحاكي (GloMoSim) لدراسة اثر التعديلات التي أجريت على بروتوكول متجه المسافة حسب الطلب الآني، وتشير النتائج إلى زيادة في نسبة الرسائل المستلمة تتراوح بين ٨٠ إلى ١٠٠ بالمائة مع زيادة في الكلفة الإضافية تتمثل في زمن تأخير الوصول وزيادة طفيفة في حزم التحكم.

ويلاحظ أن هذه الدراسة تعاني من بعض نقاط الضعف لا بد من مناقـشتها وإبـداء بعـض الملاحظات عليها:

أولا: إن هذه الدراسة قللت من احتمالية حدوث النقطة العمياء وليس منعها، إذ أن الآليـة تـم تطبيقها على العقد التي تبعد قفزتان عن العقدة المصدر فقط.

ثانيا: قد تكون العقدة الغريبة من العقد المجاورة للعقدة المصدر وتعطي معلومات صحيحة عن العقدة التي تليها من خلال رسالة الرد، وهذه حالة خاصة أخرى من النقطة العمياء لم تعالجها هذه الدراسة.

الفصل الرابع

الدراسة المقترحة لمواجهة مشكلة النقطة العمياء

٤-١ تقديم

إن البحث في مجال سرية الشبكات الآنية وبروتوكولاتها لا زال في بداياته، ويحتاج إلى مزيد من البحث والجهد، وذلك يعود لحداثة عمر هذه الشبكات من جهة وإلى خصائص تلك الشبكات من جهة أخرى.

٤-٢ الخوارزمية المقترحة لإبعاد اثر مشكلة النقطة العمياء.

تقوم هذه الخوارزمية على فرضية محدودية مصادر العقد في الشبكات اللاسلكية وقدرتها المحدودة في مجال المعالجة، ففي الحالة الطبيعية (أي بخلو الشبكة من العقد الغريبة) لا يترتب أي مجهود إضافي على العقد بعكس الخوارزميات المعقدة الأخرى التي عالجت موضوع السرية والأمان (Pirsada and Datta, ٢٠٠٤).

ويمكن تطبيقها على معظم بروتوكولات التمرير مع بعض التعديلات عليها بحسب آلية عمل كل بروتوكول.

وقد تم تطبيق الخوارزمية المقترحة في هذه الرسالة على بروتوكول متجه المسافة حسب الطلب الشبكات الآنية (AODV) ومن خلال سيناريو عمل هذا البروتوكول، وعلى النحو التالي:

أ – تقوم العقدة التي تريد أن ترسل (Source) بالبحث في جدول المسارات لديها عن مسار فعال يوصلها إلى العقدة التي تريد أن ترسل إليها (Destination).

ب- في حال وجد هذا المسار تقوم بإرسال حزمة بيانات إلى العقدة التي تليها في المسار وتقوم بتخزين عنوان العقدة التالية (Next Hop) وعنوانها في جدول خاص (Black Table) أنشأ لذلك، ثم تنتظر لفترة محددة من الوقت يجب أن تقوم العقدة التالية خلالها بتمرير حزمة البيانات.

ج- في حال تم تمرير حزمة البيانات من قبل العقدة التالية تقوم العقدة المصدر بحذف المدخل الذي تم ادخالة في (Black Table) وتواصل عملية إرسال حزم البيانات.

د- في حال انتهاء الوقت المحدد لانتظار إعادة الإرسال دون أن ترسل العقدة التالية حزمة البيانات إلى العقدة التي تليها، تقوم العقدة المصدر بحذف كل المسارات المارة بتلك العقدة.

هـ– تقوم العقدة المصدر ببث رسالة إعلان (Black Message) عن وجود نقطة عمياء في الشبكة لكافة جيرانها تحمل عنوان العقدة التالية.

و – تقوم كل عقدة استلمت رسالة الإعلان (Black Message) بالبحث في جدول المسارات لديها وتقوم بحذف المسارات التي تحتوي عنوان تلك العقدة.

ز – أما إذا كانت العقدة الغريبة عقدة وسيطة وغير مجاورة للعقدة المصدر فان هذه الوظيفة تقوم بها العقدة التي تسبقها في المسار وبنفس الآلية ويستثنى من ذلك العقدة التي تسبق الهدف التي تقوم بتسليم حزم البيانات إلى الهدف مباشرة.

ويمكن تطبيق هذه الخوارزمية على بروتوكولات التمرير الأخرى للشبكات اللاسلكية الآنية وذلك بإجراء بعض التعديلات عليها وفقا لآلية عمل كل بروتوكول.

فيمكن تطبيقها على بروتوكول المصدري الديناميكي (DSR) بطريقة أسهل وذلك لوجود آلية للتصنت في البروتوكول والمطلوب فقط تمييز رسالة الرد، ومعرفة مصدرها، فإذا كانت رسالة الرد من العقدة الهدف فلا حاجة للمراقبة ويتم إرسال حزم البيانات عبر المسار، وإلا فانه يتم اختيار مسار آخر لا يمر بالعقدة الوسيطة التي بعثت رسالة الرد(RREP)، ويتم من خلال هذا المسار التأكد من وصول حزم البيانات للعقدة الهدف باستخدام رسالة تأكيد (Acknowledgment). إذا لم يستلم المصدر وخلال فترة معينة رسالة التأكيد يقوم بحذف المسار الأول واستخدام المسار البديل.

الفصل الخامس

المحاكـــــــــــاة

٥–١ تقديم

يعتبر المحاكيان (NS٢) و (GloMoSim) من أشهر المحاكيات التي تـــستخدم فـــي المجـــالات التعليمية والأكاديمية لتقييم البروتوكولات اللاسلكية الآنية. وتستخدم المحاكيات كمرحلة أولى في عملية تطبيق البروتوكولات وتعديلاتها قبل عملية التنفيذ الفعلية والتي تتطلب كلفة مالية ومزيدا من الوقت، وكذلك بعض البرامج الإضافية الخاصة كنظم تشغيل الشبكات وباقي البروتوكولات.
يستخدم المحاكي من أجل تقييم أداء البروتوكول المقترح أو المعدل ومقارنته مع البروتوكـــول المراد إجراء التحسين عليه، وذلك بتعريضهما لنفس الظروف واستخدام عدة مقـــاييس للتقيـــيم، ويتم عادة في المحاكاة تغيير مواصفات حركة العقد وعدد العقد المصدرية والمساحة التي توجد بها عقد الشبكة وغيرها من المعاملات التي تساعد في تقييم البروتوكول من جوانبه المختلفة.

سوف نستخدم في هذه الدراسة المحاكي (GloMoSim) وذلك لإجراء المقارنات بين البروتوكول (AODV) الذي تمت إضافة عقد غريبة عليه كبروتوكول أساسي وبروتوكول (AODV) المعدل بحسب الخوارزمية المقترحة لحل مشكلة النقطة العمياء (Black Hole).

٥–٢ المحاكي (GloMoSim)

يستخدم المحاكي (GloMoSim) لمحاكاة الشبكات اللاسلكية العادية والشبكات اللاسلكية الآنيـــة. وقد تم بناء هذا المحاكي في مختبرات الحسابات المتوازية في جامعة كاليفورنيـــا فـــي لـــوس أنجلوس. يعتمد المحاكي (GloMoSim) في تصميمه على محاكي بيئـــة الأحـــداث المنفـــصلة المتوازية (PARSEC) المكتوب بلغة البرمجة (C). وقد استخدمنا في هذه الدراســـة الإصـــدار (٢,٠٣) من المحاكي (GloMoSim).
صمم المحاكي (GloMoSim) بطريقة تجعل من السهل إضافة بروتوكول جديد لأي طبقة مـــن الطبقات المكونة للمحاكي أو التعديل على البروتوكولات المرفقة معه.
يتكون المحاكي (GloMoSim) من الطبقات التالية: طبقة التطبيقات (Application Layer) وطبقة النقل (Transport Layer) وطبقة الشبكة أو التمرير (Network Routing Layer) وطبقة الوصول إلى الوسط (MAC Layer) وأخيرا الطبقة المادية (Physical/Radio Propagation Layer).

يمكن تطبيق النماذج أو البروتوكولات المرفقة مع المحاكي في كل طبقة ويمكن إضافة نماذج أو بروتوكولات جديدة من قبل الباحثين.

٥-٣ بيئة المحاكاة

قمنا بمحاكاة شبكة لاسلكية آنية مكونة من ١٥ و٢٠ و٢٥ و٣٠ و٣٥ عقدة لاسلكية متحركة تتنقل في مساحة محاكاة مربعة (١٠٠٠ ×١٠٠٠)، ولزمن محاكاة مقداره (١٠٠ ثانية) بزمن توقف مقداره (صفر و١٠) ثواني، وحركة العقد بسرعة (٠-٢٠ م/ثانية) وبمدى إرسال راديوي يبلغ (٢٥٠ متر) لكل عقدة، واستخدمنا سعة نطاق للقنوات مقدارها (٢ ميجابت/ثانية).

استخدمنا الإستراتيجية المنتظمة لتوزيع العقد (Uniform Node Placement) وذلك لتوزيع العقد اللاسلكية على مساحة المحاكاة، حيث يتم تقسيم مساحة المحاكاة إلى عدد من الخلايا يساوي عدد العقد المستخدمة في المحاكاة، ومن ثم يتم اختيار عقدة بشكل عشوائي لكل خلية من الخلايا. استخدمنا نموذج الوجهة العشوائية (Random-Waypoint Model) لحركة العقد في مساحة المحاكاة ، حيث تقوم العقدة باختيار وجهة عشوائية تقع داخل مساحة المحاكاة، ثم تتحرك باتجاه تلك الوجهة بسرعة معينة، تتوزع بشكل منتظم من صفر إلى عشرين متر لكل ثانية (٠-٢٠) وعندما تصل العقدة إلى وجهتها فإنها تتوقف لفترة من الزمن مقدارها زمن التوقف، ومن ثم تتحرك من جديد إلى وجهة أخرى.

استخدمنا (CBR) كنموذج لمصدر البيانات. واخترنا حجم حزم البيانات المرسلة ليكون (٥١٢ بايت). يستخدم المحاكي (GloMoSim) معاملا (Seed) لضمان عشوائية متنوعة في توزيع العقد على مساحة المحاكاة وفي حركة هذه العقد أثناء زمن المحاكاة، وعندما يكرر تنفيذ المحاكاة لعدة مرات يتم تغيير قيمة هذا المعامل في كل مرة. وقد قمنا بتكرار تنفيذ المحاكاة عشرة مرات وذلك لكل عدد من العقد للبروتوكول (AODV) وفي حالتين مختلفتين عند وجود عقدة غريبة واحدة وكذلك عقدتين ثم حسبنا متوسط النتائج لجميع هذه التكرارات للحصول على نتيجة المحاكاة النهائية. ثم قمنا بتكرار المحاكاة باستخدام البروتوكول (AODV) المصاب بعد إضافة التعديل عليه من اجل معالجة العقد التي أحدثت مشكلة النقطة العمياء في الحالتين لعزلها عن الشبكة. استخدمنا البروتوكول (IEEE ٨٠٢,١١) كبروتوكول التحكم في الوصول إلى الوسط

(MAC). ويبين الجدول (٥-١) البروتوكولات المستخدمة في كل طبقة من الطبقات التي يتكون منها المحاكي (GloMoSim).

جدول(٥-١)

الطبقة	البروتوكول المستخدم
التطبيقات (Application)	CBR
النقل (Transport)	UDP
التمرير (Routing)	AODV
التحكم بالوسط (MAC)	IEEE ٨٠٢,١١
المادية (Radio Propagation)	Two-Ray Ground Reflection

يبين الجدول (٥-٢) بروتوكولات التمرير المستخدمة في الدراسة

جدول(٥-٢)

الحالة	البروتوكول المستخدم
الأولى	بروتوكول (AODV) بوجود عقدة غريبة واحدة
الثانية	بروتوكول (AODV) بوجود عقدة غريبة مع إضافة التعديل
الثالثة	بروتوكول (AODV) بوجود عقدتين غريبتين
الرابعة	بروتوكول (AODV) بوجود عقدتين غريبتين مع إضافة التعديل

يبين الجدول (٥-٣) بعض الإعدادات التي استخدمت لمحاكاة بروتوكول (AODV) ولجميع الحالات التي تم تنفيذها.

الجدول (٥-٣)

المتغير	قيمته
مدة فعالية المسار	١٠ ثواني
مدة انتظار رسالة الرد بين عقدتين متجاورتين	٤٠ ملي ثانية
مدة انتظار العقدة المصدر للرد من العقدة الهدف	٢١٠٠ ملي ثانية

ويبين الجدول (٥-٤) بعض المعاملات التي استخدمت لمحاكاة بروتوكولات التمرير لكل الحالات التي تم تنفيذها.

الجدول (٥-٤)

المتغيرات	القيم
زمن المحاكاة	١٠٠ ثانية
عدد العقد في الشبكة	١٥،٢٠،٢٥،٣٠،٣٥
زمن التوقف	٠،١٠ ثانية
مساحة منطقة المحاكاة	١٠٠٠X١٠٠٠ م
السرعة الدنيا للعقد ضمن مساحة المحاكاة	٠ م/ ثانية
السرعة القصوى للعقد	٢٠ م/ ثانية

٥-٤ عمل المحاكي

يحتاج المحاكي عند تنفيذه إلى قراءة المدخلات من ملف الإعداد (config.in). يحتوي ملف الإعداد قيم المعاملات التي تحدد بيئة المحاكاة، كعدد العقد المستخدمة ومساحة المحاكاة وزمن المحاكاة والبروتوكول المستخدم في كل طبقة من الطبقات والإستراتيجية المستخدمة لتوزيع العقد على مساحة المحاكاة ونموذج حركة العقد وسرعتها وغيرها من المعاملات اللازمة لتعريف بيئة المحاكاة. ويحدد ملف الإعداد كذلك نوع بروتوكول التمرير المستخدم وملف مصادر البيانات

(app.conf). أما ملف مصادر البيانات فيحدد عناوين العقد المرسلة (Sources) والعقد الهدف (Destinations) والبروتوكول المستخدم في طبقة التطبيقات (Application) بالإضافة إلى حجم حزم البيانات المرسلة ووقت البدء في عملية الإرسال ووقت التوقف عن الإرسال وذلك لكل عقدة مصدرية.

بعد كل تنفيذ للمحاكاة ينتج ملف مخرجات (statistic) يحتوي معلومات إحصائية لكل عقدة في الشبكة اللاسلكية الآنية، إذ يعطي المحاكي إمكانية الحصول على معلومات إحصائية وافية لكل طبقة من الطبقات ولكل عقدة. وقد تم تعديل بروتوكولات التمرير بربطها ببرنامج اكسل، وذلك لوضع إحصائيات النتائج في ملف اكسل يتم إنشاؤه مباشرة بعد كل محاكاة، مما يسهل معالجة الإحصائيات الناتجة من عميلة المحاكاة. ينحصر اهتمامنا في هذه الدراسة بالمعلومات الإحصائية الخاصة بطبقتي التطبيقات والتمرير. نستطيع من خلال الإحصائيات الخاصة بطبقة التطبيقات أن نحسب متوسط عدد حزم البيانات المرسلة وعدد الحزم المستلمة لكل التجارب التي تم تنفيذها. ونستطيع أيضا أن نحسب نسبة تسليم الحزم وإنتاجية الشبكة (Throughput) وعدد الحزم المحذوفة وكلفة تمرير حزم البيانات من خلال المعلومات الإحصائية الخاصة بطبقة التمرير.

٥-٥ مقاييس تقييم الأداء المستخدمة

استخدمنا في هذه الدراسة مجموعة من المقاييس لتقييم أداء البروتوكول المقترح ومقارنته بالبروتوكول الأصلي المعدل، والمقاييس هي: نسبة تسليم الحزم (Packet Delivery Ratio)، وعدد الحزم المحذوفة وإنتاجية الشبكة. وفيما يلي وصف لهذه المقاييس:

٥-٥-١ نسبة تسليم الحزم (Packet Delivery Ratio)

وهي النسبة بين العدد الكلي لحزم البيانات المستلمة من قبل العقد الهدف إلى عدد حزم البيانات المفروض استلامها (Liao, ٢٠٠٥)، حيث أن العدد الكلي لحزم البيانات المفروض استلامها هو عدد الحزم المرسلة من قبل المصادر. وتمثل هذه النسبة كفاءة البروتوكول في تسليم البيانات إلى وجهاتها داخل الشبكة.

٥-٥-٢ الإنتاجية (Throughput)

وهي عدد الرسائل أو عدد البيانات الثنائية (Bits) التي يتم التعامل معها من قبل الشبكة ويعتبر مجموعها مقياسا لإنتاجية الشبكة بشكل عام.

٥-٥-٣ عدد الحزم المسقطة (Dropped Packets)

وهو عدد الحزم المسقطة والتي يتم حذفها بسبب انتهاء المدة الزمنية المحددة لهـا أو بـسبب حدوث تصادم (Collision). فقد استخدمنا في هذه الدراسة عدد العقد التي تم حذفها بسبب العقـد التي تسببت في حدوث مشكلة ألنقطة العمياء في الشبكة كأحد مقاييس كفاءة البروتوكول المعدل.

٥-٦ تحليل نتائج محاكاة البروتوكولات

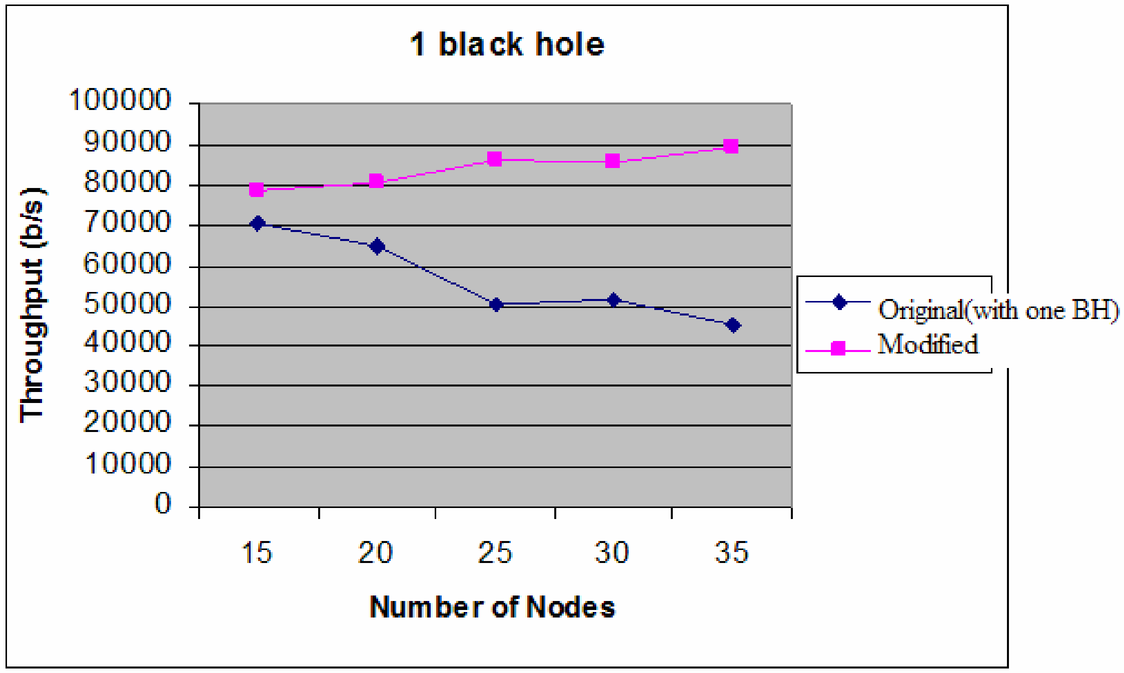
سنتناول في هذا البند نتائج محاكاة نسخة بروتوكول (AODV) التي تم إدخال العقد الغريبة عليها بالمقارنة مع النسخة المزودة بخوارزمية الكشف والعزل لتلك العقد في الشبكة. تم تصنيف نتائج المحاكاة حسب مجموعة من المعاملات التي تؤثر على مقاييس تقييم الأداء، وهي عـدد العقـد الغريبة في الشبكة وعدد العقد كلها مع تثبيت مساحة المحاكاة وعدد المصادر.

٥-٦-١ تأثير زيادة عدد العقد من ١٥ إلى٣٥ عقدة لزمن التوقف الذي يساوي صفراً

أولا:

١- اثر زيادة عدد العقد على إنتاجية الشبكة بوجود عقدة غريبة واحدة

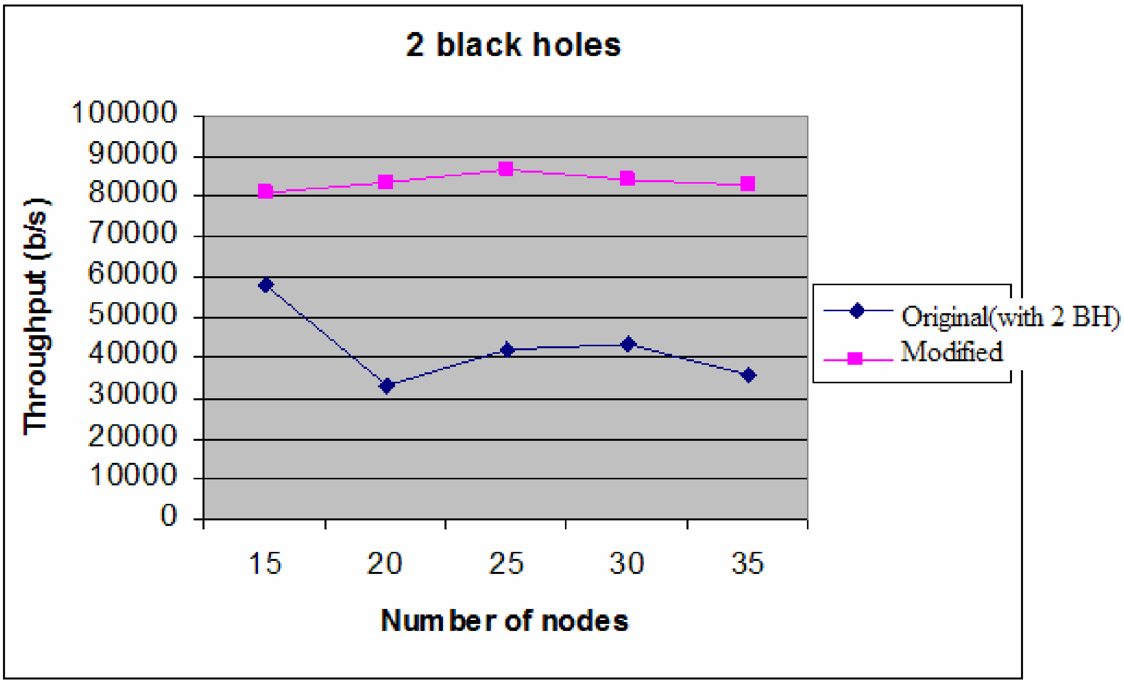
أظهرت نتائج المحاكاة معدل نسب التحسين للبروتوكول المقترح مقارنة بالبروتوكول الأصلي المعدل زيادة ٤٩ بالمائة تقريبا في إنتاجية الشبكة، ويلاحظ من الشكل انه بازدياد عدد العقد فان إنتاجية البروتوكول قد زادت بنسبة ١٤ بالمائة للبروتوكول المقترح، بينما انخفضت النسبة بشكل كبير في البروتوكول الأصلي المعدل بلغت ٣٥ بالمائة، وكما هو مبين في الشكل (٥-١).



الشكل (٥-١) العلاقة بين الإنتاجية وعدد العقد بوجود عقدة غريبة واحدة لزمن التوقف صفر ثانية.

٢- اثر زيادة عدد العقد على إنتاجية الشبكة بوجود عقدتين غريبتين

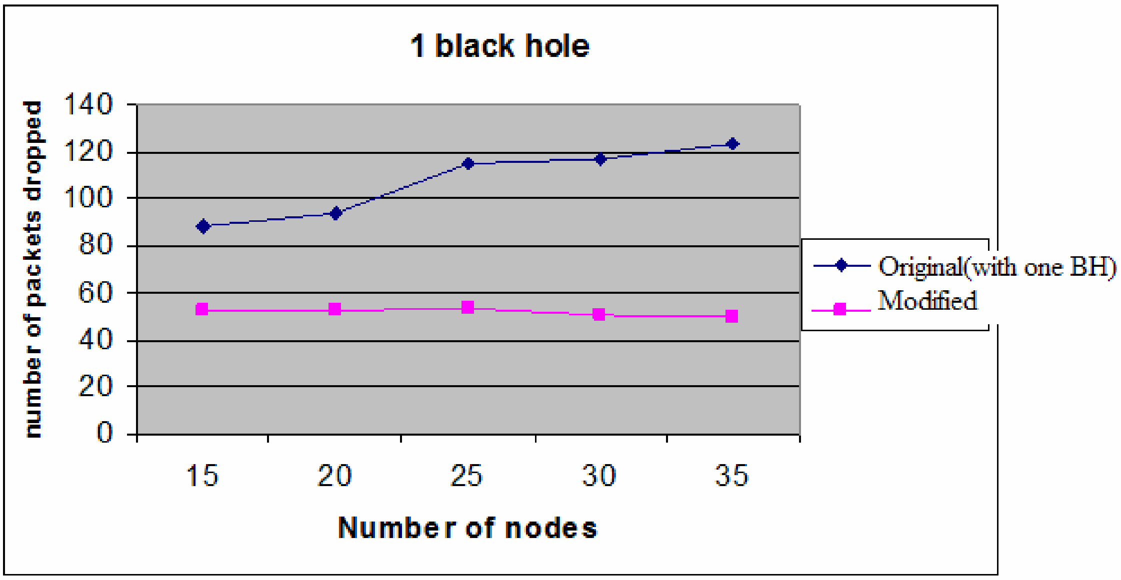
أما بوجود عقدتين غريبتين فان معدل نسبة التحسين بلغت ٩٦ بالمائة تقريبا للبروتوكول المقترح وقد ازدادت نسبة التحسين للبروتوكول المقترح بنسبة طفيفة مع ازدياد عدد العقد (١ بالمائة تقريبا) أي أنها حافظت على مستواها تقريباً، بينما انخفضت بنسبة ٢٧ بالمائة للبروتوكول الأصلي المعدل ولنفس الظروف كما هو مبين في الشكل (٥-٢).



الشكل (٥-٢) العلاقة بين الإنتاجية وعدد العقد بوجود عقدتين غريبتين لزمن التوقف صفر ثانية.

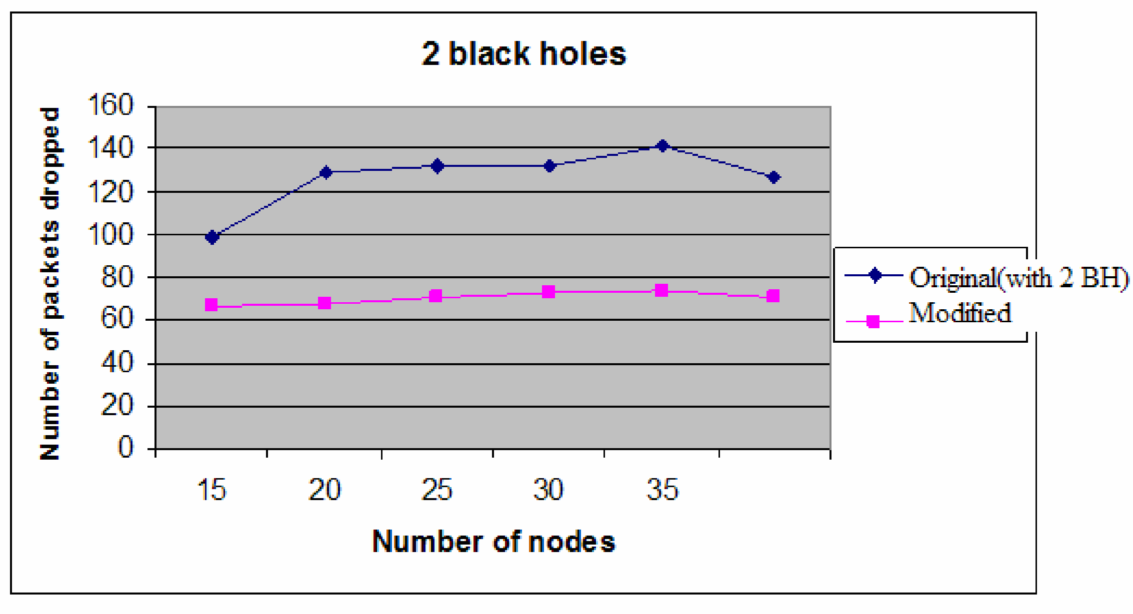
ثانيا:

١- اثر زيادة العقد على عدد الحزم المسقطة بوجود عقدة غريبة واحدة: تبين نتائج المحاكاة أن معدل نسبة التحسين (النقص) في عدد الحزم المحذوفة للبروتوكول المقترح مقارنة بالبروتوكول الأصلي المعدل بلغت ٤٠ بالمائة تقريبا، وقد نقص عدد الحزم المسقطة بشكل طفيف للبروتوكول المقترح عند زيادة عدد العقد بوجود عقدة غريبة واحده بينما زادت بنسبة ٣٩ بالمائة للبروتوكول الأصلي ولنفس الظروف كما هو مبين في (٥-٣).



الشكل (٥-٣) العلاقة بين عدد الحزم المسقطة وعدد العقد بوجود عقدة غريبة لزمن التوقف صفر ثانية.

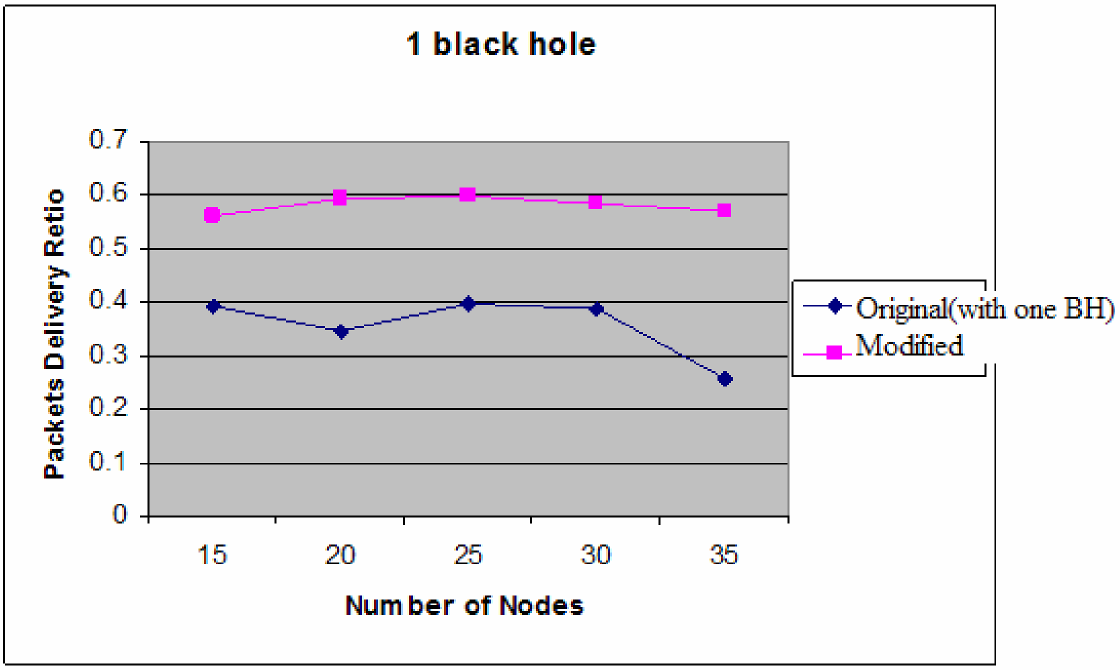
٢- أما بوجود عقدتين غريبتين فقد بلغت نسبة التحسين للبروتوكول المقترح مقارنة بالبروتوكول الأصلي المعدل ٤٥ بالمائة، فيما زادت نسبة العقد المسقطة بنسبة ١ بالمائة للبروتوكول المقترح بازدياد عدد العقد بينما زادت نسبتها في البروتوكول الأصلي المعدل إلى ٤٣ بالمائة و لنفس الظروف وكما هو مبين في الشكل (٥-٤).



الشكل (٥-٤) يبين العلاقة بين عدد العقد وعدد الحزم المسقطة بوجود عقدتين غريبتين لزمن التوقف صفر ثانية.

ثالثا:

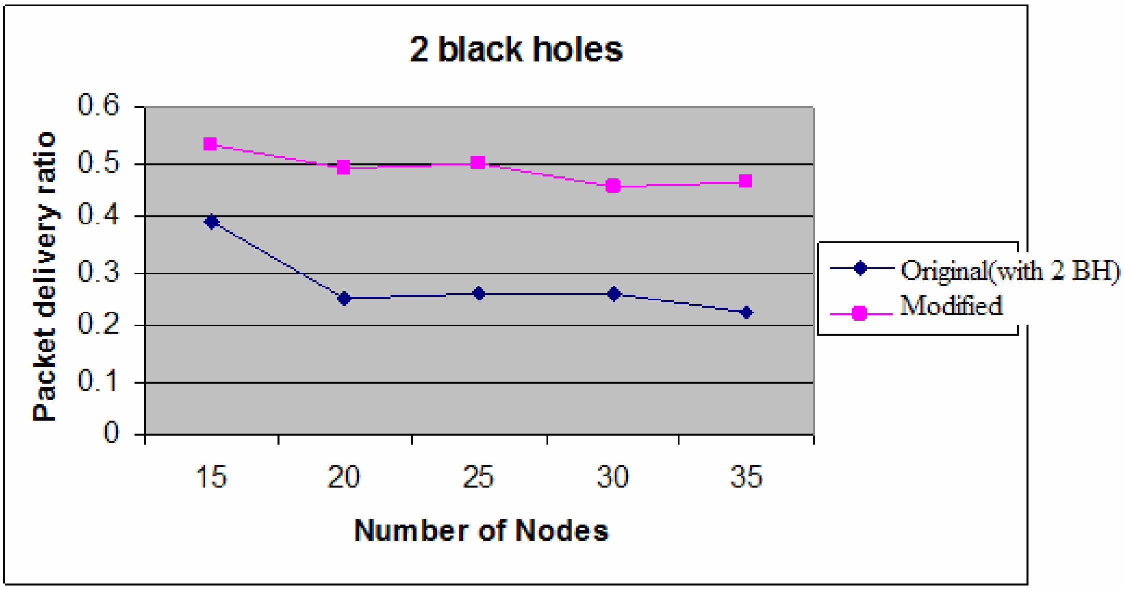
١- اثر زيادة العقد على نسبة تسليم الحزم بوجود عقدة غريبة واحدة: نلاحظ أن معدل نسبة التحسين في تسليم الحزم للبروتوكول المقترح مقارنة بالبروتوكول الأصلي المعدل بلغت ٤١ بالمائة تقريبا وان البروتوكول المقترح قد حافظ على نسب تسليم الحزم تقريبا مع زيادة عدد العقد بينما نقص نسبة التسليم للبروتوكول الأصلي المعدل بنسبة ٣٧ بالمائة وكما هو واضح في الشكل (٥-٥).



الشكل (٥-٥) العلاقة بين عدد العقد ونسبة تسليم الحزم عند وجود عقدة غريبة واحدة لزمن التوقف صفر ثانية.

٢- اثر زيادة العقد على نسبة تسليم الحزم بوجود عقدتين غريبتين

أما بوجود عقدتين غريبتين فان معدل نسبة التحسين للبروتوكول المقترح مقارنة بـــالبروتوكول الأصلي المعدل بلغت ٤٣ بالمائة، وقد نقصت نسبة تسليم الحزم فـــي البروتوكـــول المعـــدل ١ بالمائة فيما نقصت بنسبة ٤٣ بالمائة تقريبا للبروتوكول الأصلي المعدل وكما في الشكل (٥-٦).



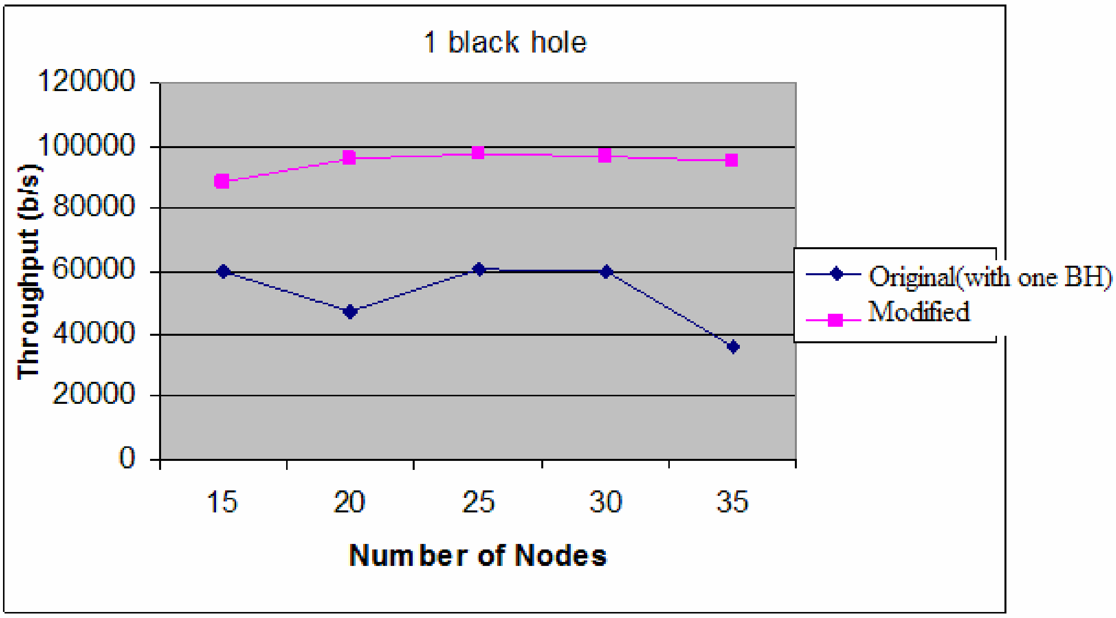
الشكل (٥-٦) العلاقة بين عدد العقد ونسبة تسليم الحزم بوجود عقدتين غريبتين لزمن التوقف صفر ثانية.

٥-٦-٢ تأثير زيادة عدد العقد من ١٥ إلى٣٥ عقدة لزمن التوقف الذي يساوي ١٠ ثوانيً

أولا :

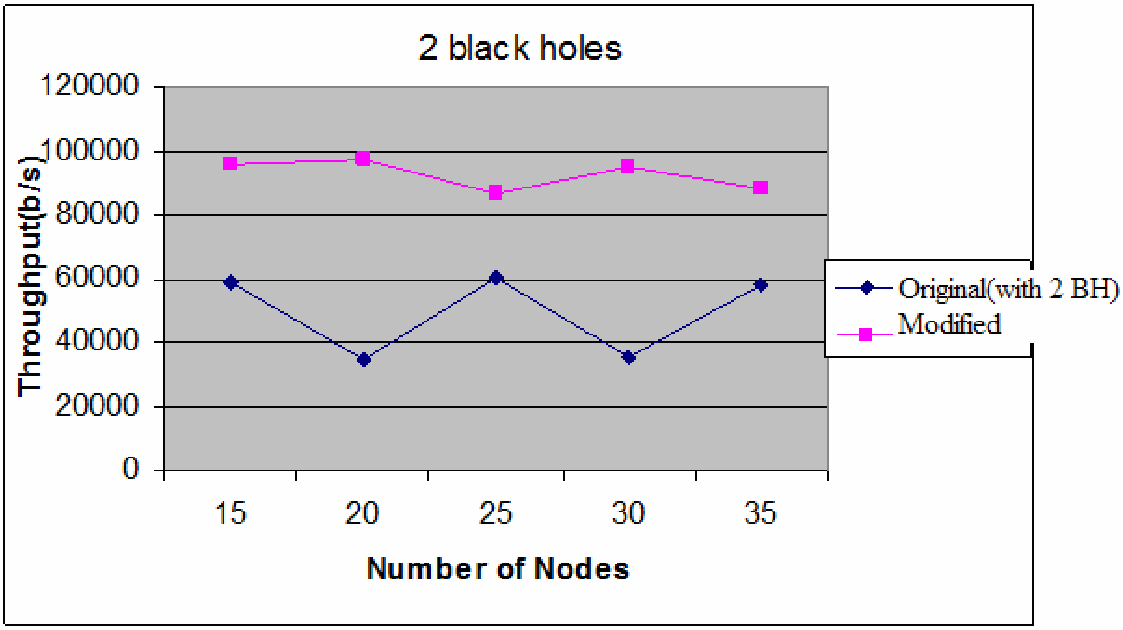
اثر عدد العقد على إنتاجية الشبكة

١- أظهرت نتائج المحاكاة بوجود عقده غريبة في الشبكة تحسنا لمعدل نسبة الإنتاجية للبروتوكول المقترح مقارنة بالبروتوكول الأصلي بنسبة ٨٠ بالمائة، ونقصا في نسبة الإنتاجية بازدياد عدد العقد للبروتوكول المعدل بنسبة ٧ بالمائة في حسب نقصت نسبة الإنتاجية للبروتوكول المعدل بنسبة ٣٩ بالمائة للبروتوكول الأصلي تقريبا وكما في موضح الشكل (٥-٧).



الشكل (٥-٧) علاقة إنتاجية الشبكة بعدد العقد بوجود عقدة غريبة واحدة عند التوقف لعشرة ثواني.

٢- أما بوجود عقدتين غريبتين فان معدل نسبة التحسين في الإنتاجية للبروتوكول المعدل مقارنة بالبروتوكول الأصلي قد وصلت إلى ٨٧ بالمائة، وقد زادت نسبة التحسين في الإنتاجية للبروتوكول الأصلي ٨ بالمائة بزيادة عدد العقد بينما زادت نسبة الإنتاجية للبروتوكول الأصلي بنسبة ٧ بالمائة للبروتوكول الأصلي ولنفس الظروف وكما هو واضح في الشكل (٥-٨)



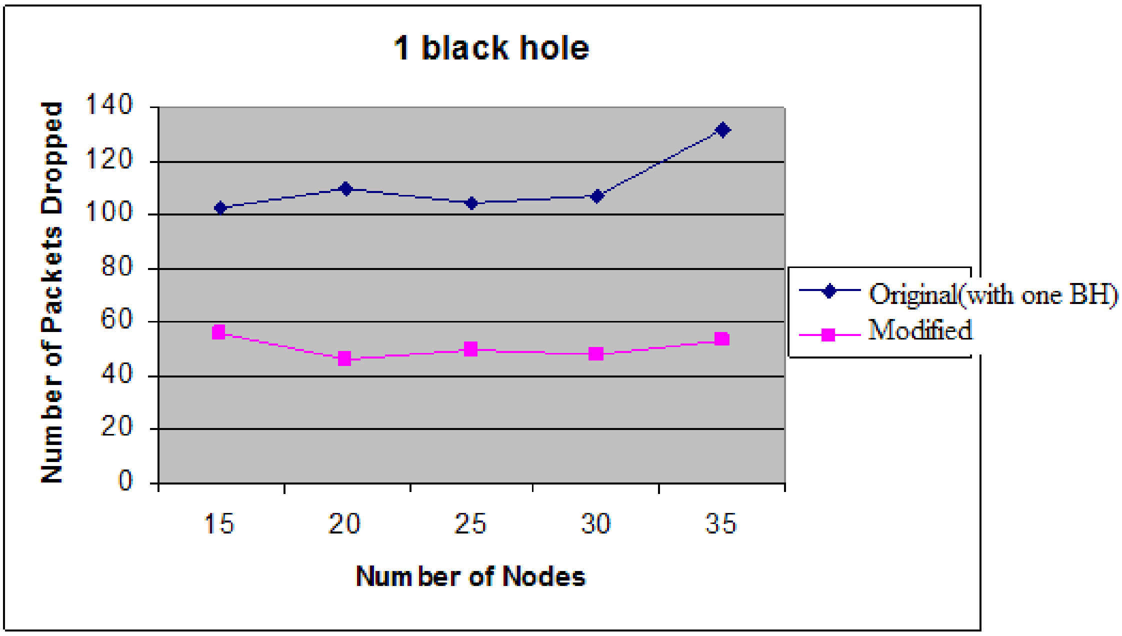
الشكل (٥-٨) علاقة إنتاجية الشبكة بعدد العقد بوجود عقدتين غريبتين عند التوقف لعشرة ثواني.

ثانيا

اثر زيادة العقد في الشبكة على عدد الحزم المسقطة (الضائعة)

١- اثر زيادة عدد العقد على نسبة الحزم المسقطة بوجود عقدة غريبة في الشبكة

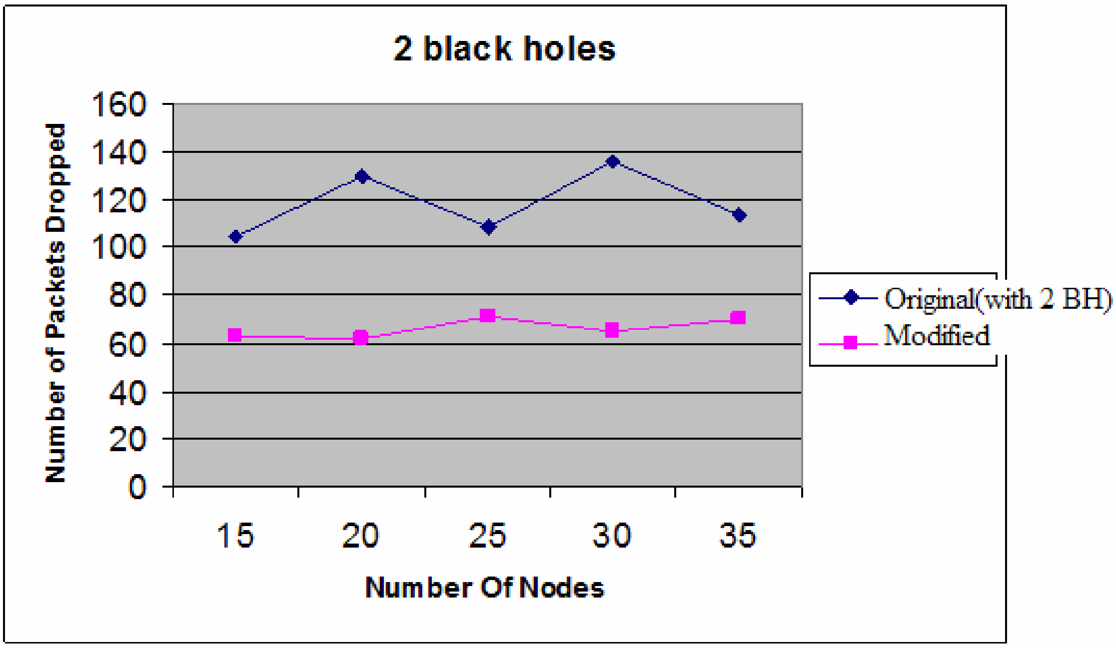
تشير نتائج المحاكاة بان نسبة التحسين (التقليل) في معدل الحزم المسقطة للبروتوكول المعدل بوجود عقدة غريبة واحدة مقارنة بالبروتوكول الأصلي بلغت ٦٠ بالمائة، وكما تشير أن نسبة الحزم الضائعة للبروتوكول المعدل بقيت ثابتة تقريبا بزيادة عدد العقد في الشبكة بينما زادت النسبة للبروتوكول الأصلي بمقدار ٢٨ بالمائة بزيادة عدد العقد وكما هو واضح في الشكل (٥-٩).



الشكل (٥-٩) العلاقة بين عدد العقد وعدد الحزم الضائعة بوجود عقده غريبة واحدة لـزمن التوقف عشرة ثواني.

٢- اثر زيادة عدد العقد في الشبكة على عدد الحزم الضائعة بوجود عقـدتين غـريبتين فـي الشبكة.

تشير نتائج المحاكاة أن معدل نسب التحسين (النقص) في عدد الحزم المـسقطة للبروتوكـول المعدل مقارنة بالبروتوكول الأصلي بلغت ٧٠ بالمائة، وتشير إلى زيادة طفيفة في البروتوكول المعدل بازدياد عدد العقد، أما البروتوكول الأصلي فان نسبة الزيادة غير منتظمة وقد بلغت ٨ بالمائة مع زيادة عدد العقد وكما هو مبين في الشكل (٥-١٠).

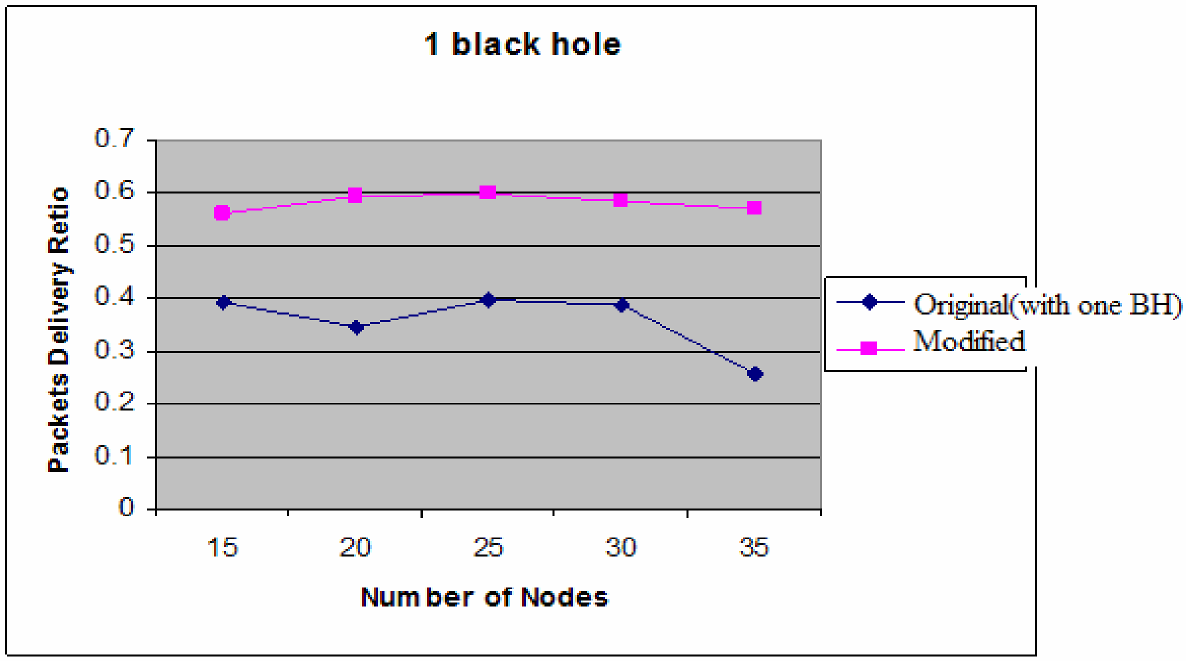


الشكل (٥-١٠) علاقة عدد العقد بعدد الحزم الضائعة بوجود عقدتين غريبتين في الشبكة لزمن التوقف عشرة ثواني.

ثالثا

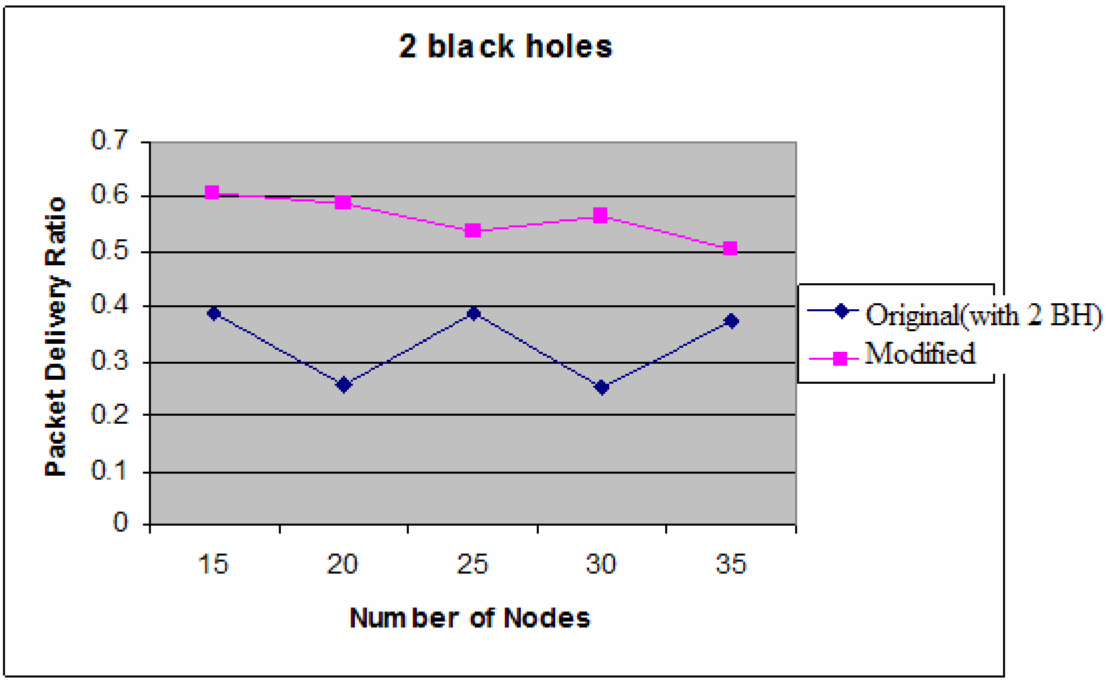
اثر زيادة العقد في الشبكة على نسبة تسليم الحزم

١- تشير نتائج المحاكاة أن معدل نسبة التحسين في تسليم الحزم بوجود عقدة غريبة واحدة للبروتوكول المعدل مقارنة بالبروتوكول الأصلي بلغت ٦٣ بالمائة وتشير إلى زيادة طفيفة في نسبة تسليم الحزم للبروتوكول المعدل مع زيادة العقد، بينما انخفاض تلك النسبة للبروتوكول الأصلي ٣٥ بالمائة مع زيادة عدد العقد وكما يبين الشكل (٥-١١).



الشكل (٥-١١) علاقة عدد العقد في الشبكة بنسبة تسليم الحزم بوجود عقـدتين غـريبتين لزمن التوقف عشرة ثواني.

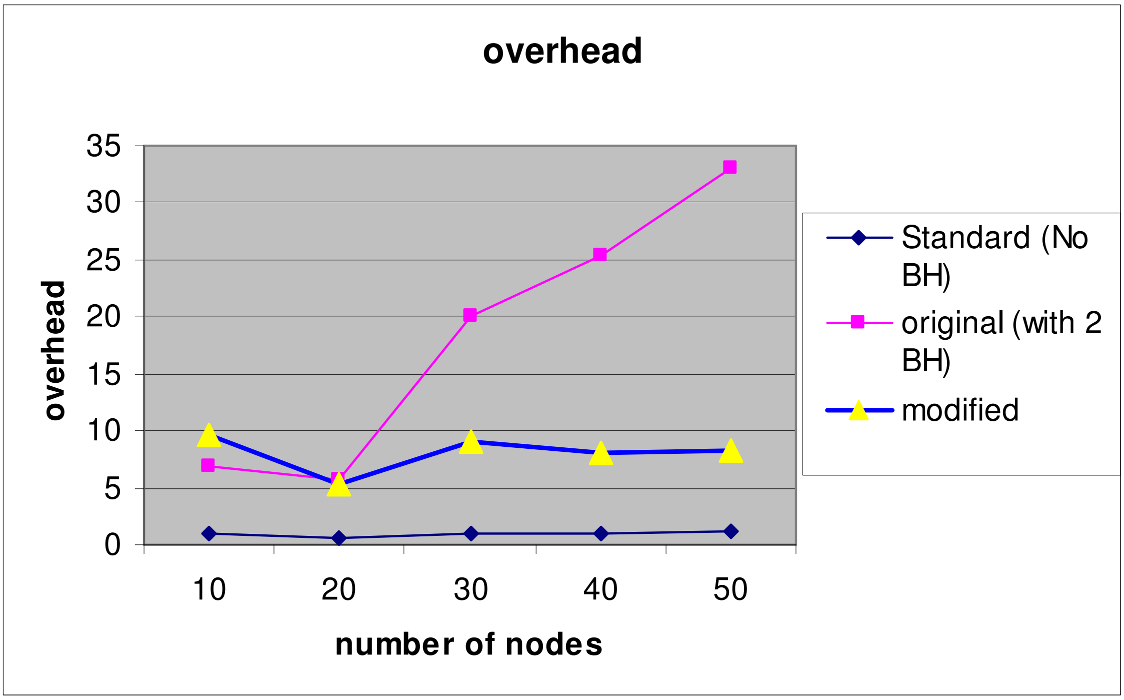
٢- أما بوجود عقدتين غريبتين فان نتائج المحاكاة تبين أن معدل نسبة التحسين في تسليم الحزم للبروتوكول المعدل مقارنة بالبروتوكول الأصلي بلغت ٦٩ بالمائة، وقد انخفضت نسبة التسليم للبروتوكول المعدل بنسبة ١٧ بالمائة مع زيادة عدد العقد بينما انخفضت النسبة للبروتوكول الأصلي بنسبة طفيفة وكما هو مبين في الشكل (٥-١٢).



الشكل (٥-١٢) علاقة عدد العقد في الشبكة بنسبة تسليم الحزم بوجود عقدتين غريبتين لزمن التوقف عشرة ثواني.

٥-٦-٣ الكلفة الإضافية (Overhead)

تشير نتائج المحاكاة إلى زيادة واضحة في الكلفة الإضافية للبروتوكول المعدل مقارنة بالبروتوكول الأصلي، وكذلك تناقص بشكل كبير مقارنة بالبروتوكول الأصلي بعد إضافة العقد الغريبة عليه وبزيادة عدد العقد في الشبكة، وهذا تحدي يواجه جميع الدراسات التي قدمت في تامين بروتوكولات التمرير في الشبكات اللاسلكية الآنية، والشكل (٥-١٣) يبين علاقة الكلفة الإضافية بعدد العقد لكل من البروتوكولات الثلاث.



الشكل (٥-١٣) الكلفة الإضافية في البروتوكول المعدل مقارنـــة مـــع البروتوكـــول الأصـــلي والبروتوكول الذي يحتوي على عقدتين غريبتين.

الفصل السادس

الاستنتاجات

٦-١ تحليل نتائج المحاكاة

قمنا في هذه الدراسة بتعديل بروتوكول متجه المسافة حسب الطلب الآني بغرض تجنب حدوث النقطة العمياء، وتمت مقارنة البروتوكول المعدل مع البروتوكول الأصلي بعد إضافة عقد غريبة عليه باستخدام المعايير التالية: نسبة تسليم الحزم وعدد الحزم الضائعة والكلفة الإضافية.

ولتقييم مدى نجاح التعديلات المضافة على بروتوكول متجه المسافة حسب الطلب الآني قمنا باستخدام طريقة المحاكاة معتمدين في ذلك على المحاكي (Glomosim) ودرسنا أداء البروتوكول قبل وبعد التعديلات باستخدام المعايير المذكورة سابقاً وذلك بتعريض البروتوكول الأصلي والذي يعاني من وجود مشكلة النقطة العمياء والبروتوكول المعدل إلى نفس الظروف من حيث الحركة والسرعة وعدد العقد وزمن التوقف وعدد المصادر.

وقد حصلنا على النتائج التالية :

بالنسبة لعدد المسارات المخزنة في ذاكرة العقد فقد انخفض انخفاضا كبيراً في البروتوكول المعدل مقارنة بالبروتوكول الأصلي، فعند السرعة (٥م/ثا) تراوحت نسبة التحسين بين (٧٦,٨٢%) و(٩٤,٦٠%)، أما عند السرعة (١٠م/ثا) تراوحت نسبة التحسين بين (٦٢%) و (٩٠%)، وعند السرعة (٢٠م/ثا) تراوحت نسبة التحسين بين (٦٥%) و (٨٦%)، أي تم توفير مساحات من ذاكرة العقد بالنسب المئوية السابقة كانت مستخدمة بلا فائدة.

من حيث نسبة تسليم الحزم أظهر البروتوكول المعدل نسبة تسليم أعلى من البروتوكول الأصلي فعند السرعة (٥م/ثا) تراوحت نسبة التحسين بين (٤,١%) و (١٤,٤٠%)، أما عند

السرعة (١٠م/ثا) تراوحت نسبة التحسين بين (٤,٣%) و (١٥,٢٣%) وعند السرعة (٢٠م/ثا) تراوحت نسبة التحسين بين (٥,٤٣%) و (٢١,٩٥%) .

من ناحية عدد الحزم الضائعة أظهر البروتوكول المعدل تحسناً ملحوظاً حيث قل عدد الحزم الضائعة بالمقارنة مع البروتوكول الأصلي، فعند السرعة (٥م/ثا) تراوحت نسبة التحسين بين (٣٤,١٤%) و (٥٤,٥٤%)، أما عند السرعة (١٠م/ثا) تراوحت نسبة التحسين بين (٣٢,٨٨%) و (٣٥,٤٤%)، وعند السرعة (٢٠م/ثا) تراوحت نسبة التحسين بين (٣٤,٩٢%) و (٥١,١٠%) أي تم التقليل من ضياع الحزم بالنسب المئوية السابقة .

تم التقليل أيضاً من عدد الحزم المنقذة في البروتوكول المعدل بالمقارنة مع البروتوكول الأصلي فعند السرعة (٥م/ثا) تراوحت نسبة التحسين بين (١٦,١٧%) و (٥٧,٣٧%)، أما عند السرعة (١٠م/ثا) تراوحت نسبة التحسين بين (١٥,٨٤%) و (٥١,٦٥%) وعند السرعة (٢٠م/ثا) تراوحت نسبة التحسين بين (١٥,٥٨%) و (٥٤,٧٩%).

من ناحية عدد المسارات المقطوعة أظهر البروتوكول المعدل تحسناً ملحوظاً حيث قل استخدام المسارات المقطوعة بالمقارنة مع البروتوكول الأصلي، فعند السرعة (٥م/ثا) تراوحت نسبة التحسين بين (٢١,٦٠%) و (٣٩,٧٢%)، أما عند السرعة (١٠م/ثا) تراوحت نسبة التحسين بين (١٩,٤٥%) و (٢٦,٩٥%)، وعند السرعة (٢٠م/ثا) تراوحت نسبة التحسين بين (٢٠%) و (٤٢,٩٩%)، أي تم التقليل من استخدام المسارات المقطوعة بالنسب المئوية السابقة.

أما بالنسبة للكلفة الإضافية فقد قلت في البروتوكول المعدل بالمقارنة مع البروتوكول الأصلي في بعض الحالات وزادت في أحيان أخرى، فعند السرعة (٥م/ثا) نقصت الكلفة الإضافية بنسبة (٤١,٦٦%) لزمن التوقف (٩٠٠ ثانية) ونقصت أيضاً بنسبة (٤٢,٥٧ %) لزمن التوقف (٠ ثانية)، أما عند السرعة (١٠م/ثا) نقصت الكلفة الإضافية بنسبة (١٥,٥٥%) لزمن التوقف (٩٠٠ ثانية) وعند السرعة (٢٠ م/ثا) نقصت هذه الكلفة بنسبة (١٨,٧٥ %) لزمن التوقف (٩٠٠ ثانية)، بينما زادت عند السرعة (١٠ م/ثا) لزمن التوقف (٠ ثانية) بنسبة (٦,١٩%) ، وعند السرعة (٢٠م/ثا) فقد زادت بنسبة (١١,٧٢%) لزمن التوقف (٠ ثانية).

٦-٢ العمل المستقبلي

يمكن تحسين أداء البروتوكول المعدل بإضافة التعديلات التالية :

١. التقليل من الكلفة الإضافية في البروتوكول المعدل وذلك بعدم نشر رسالة الخطأ في الشبكة والاكتفاء بإرسالها إلى المصادر المتضررة بانقطاع مسار ما.

٢. تغيير استراتيجية اختيار مسار من ذاكرة المسارات بحيث تختار دائما المسار الأسرع بدل اختيار المسار الأقصر ومعيار السرعة هنا هو الحداثة .

٣. إلغاء توليد رسالة خطأ نتيجة فقدان رسالة جواب المسار وذلك لوجود عدة رسائل جواب مسار سترد إلى المصدر .

٤. إذا لم تستطع عقدة وسيطة أن توصل حزمة المعطيات إلى العقدة الوسيطة التالية فإنها تبحث في ذاكرتها عن مسار إلى هدف هذه الحزمة وإذا لم تجد مساراً فإنها ستحذفها، هنا نقترح ألا تحذف هذه الحزمة وأن تولد رسالة طلب مسار إلى هذا الهدف وبعد العثور على مسار ترسل الحزمة إلى هدفها مما قد يزيد من نسبة تسليم الحزم.

٥-٧ الدراسات المستقبلية

سنقوم بعدة دراسات تهدف إلى تقليل الكلفة الإضافية أولا ومن ثم تحسين أداء البروتوكول المقترح بربطه بآليات جديدة للتحكم بدخول العقد إلى الشبكة لتشكيل تحسين بشكل عمودي على بروتوكول متجه المسافة حسب الطلب الآني (AODV) لجعله بروتوكولا أكثر أمنا ضد الاعتداءات المحتملة التي تواجهه.

المراجع:

١- Deng, H., Li, W., and Agrawal, D. P., **Routing Security in Wireless Ad Hoc Networks**, IEEE Communications Magazine, Vol. ٤٠, Issue ١٠ October ٢٠٠٢. pp ٧٠–٧٥.

٢- Mukherjee, A., Bandyopadhyay, S., and Saha, D., **Location Management and Routing in Mobile Wireless Networks**, Artech House, Boston ٢٠٠٣.

٣- Mir, R. N., and Wani, A. M., **Distributed Routing in Ad Hoc Networks,** Proc. of the TENCON ٢٠٠٣, Convergent Technologies for Asia-Pacific Region, Vol.٣, ٢٠٠٣. pp ١٠٩١ – ١٠٩٥.

٤- Gavini, S., **Detecting Packet- Dropping Faults in Mobile Ad Hoc Networks** Master thesis, Washington State University, December ٢٠٠٤.

٥-Liao, L., **Group Key Agreement for Ad Hoc Networks.** Master thesis, Ruhr-University Bochum, Germany ٢٠٠٥.

٦- Yi, S., Naldurg, P., and. Kravets, R., **Security-aware Ad Hoc Routing for Wireless Networks,** Proc. of the ٢nd ACM Symposium on Mobile Ad Hoc Networking and Computing, October ٢٠٠١, pp. ٢٩٩–٣٠٢

٧- Johnson, D. B., and Maltz, D.A., **Dynamic Source Routing in Ad Hoc Wireless Networks**, Mobile Computing, Imielinski. T and Korth, H. (Editors), Kluwer Academic Publishers, ١٩٩٦, pp. ١٥٣–١٨١.

٨- Perkins, C. E., and Royer, E. M., **The Ad Hoc On-Demand Distance-Vector Protocol**, Adhoc Networking, Perkins, C. E. (editor), Addison-Wesley Publisher, ٢٠٠١.

٩- Anjum, F., and Mouchtaris, P., **Security for Wireless Ad Hoc Networks.** John Wiley & Sons, Inc. Hoboken., New Jersey ٢٠٠٧.

١٠- Ning, P., and Kun, S., **How to Misuse AODV**, Proc. of the Man and Cybernetics Society Information Assurance Workshop, IEEE June ٢٠٠٣. pp ٦٠-٦٧.

١١-Awerbuch, B., Holmer, D., Nita-Rotaru, C., and Rubens, H., **An On-Demand Secure Routing Protocol Resilient to Byzantine Failures**, Proc. of the ١st ACM workshop on Wireless security Atlanta. ٢٠٠٢. pp. ٢١-٣٠.

١٢-Awerbuch, B., Curtmola, R., Holmer, D., Nita-Rotaru, C., and Rubens, H., **Mitigating Byzantine Attacks in Ad Hoc Wireless Networks**, Proc. of the SecureCom'٠٥, Georgia, USA. September ٢٠٠٥. pp ٣٢٧-٣٣٨.

١٣-Marti, S., Giuli,T. J., Lai, K., and Baker, M., **Mitigating Routing Misbehavior in Mobile Ad Hoc Networks**, Proc. of the Sixth annual ACM/IEEE International Conference on Mobile Computing and Networking, ٢٠٠٠, pp. ٢٥٥–٢٦٥.

١٤- Pervaiz, M.O., Cardei, M., and Wu, J.**, Routing Security in Ad Hoc Wireless Networks**, Department of Computer Science and Engg, Florida Atlantic University. ٢٠٠٥.

١٥- Pirsada, A., and Datta, A., McDonald, C., **Propagating Trust in Ad-hoc Networks for Reliable Routing,** Proc. of the International Workshop on Wireless Ad-hoc Networks, IEEE ٢٠٠٤, pp. ٥٨–٦٢.

١٦- Tamilselvan, L., and Sankaranarayanan, V.**, Prevention of Blackhole Attack in MANET.** Proc. of the ٢nd International Conference on Wireless Broadband and Ultra Wideband Communications, (AusWireless ٢٠٠٧). Sydney. Australia. IEEE ٢٠٠٧. pp. ٢١-٢٦.

١٧- Perkins, C. E., Belding-Royer, E. M., and Das, S. R., **Internet draft-ietf-manet-aodv-١٣.txt**, http://www.ietf.org/ietf/١id-abstracts.txt. ٢٠٠٣, ٢٠٠٣.

١٨- Kong, J., Hong, X., Yi, Y. Park, J-S., Liu, J., and Gerla, M., **A secure Ad Hoc Routing Approach Using Localized Self-Healing Communities**. Proc. of the ٦th ACM Int. symposium on Mobile ad hoc networking and computing (MobiHoc'٠٥). May ٢٠٠٥. pp. ٢٥٤-٢٦٥.

١٩- Khalili, A., Katz, J. A, and Arbaugh, W. A. **Toward Secure Key Distribution in Truly Ad-Hoc Networks**. Proc. of the Symposium on Applications and the Internet Workshops (SAINT-w'٠٣), IEEE ٢٠٠٣, pp. ٣٤٢-٢٤٦.

٢٠- Lin, T., **Mobile Ad-hoc Network Routing Protocols**: Methodologies and Applications, Ph.D. thesis, Virginia Polytechnic Institute and State University, ٢٠٠٤.

٢١- عبد الله، فيصل، **الاكتشاف المبكر لانقطاع المسارات عنـــد المـــصادر فـــي بروتوكـــول التمرير المصدري الديناميكي**، رسالة ماجستير(غير منشوره)، جامعة آل البيت، الأردن ٢٠٠٦.

Abstract

Mobile ad hoc networks are infrastructure-less wireless networks, where each node of the network can be a source, a destination and a router for the remaining nodes. These networks can suffer from several types of attacks including the black hole attack, where the black hole node responds to route requests, but it does not forward packets to their destination.

In this thesis, we propose an algorithm for handling the black hole problem. Every node in a route must be sure that the next node forwards packets on the path to the destination. A node waits for a specific time, and if it does not hear the next node forwarding the packet it assumes that the next node is a malicious node. It removes all routes that contain that node from its routes table and it sends a black hole message to all neighbors. The neighbors remove the routes that include the black hole node, and forward the notification. This process is repeated. We use the GloMoSim simulator to compare the original AODV with one and two black hole with a version of AODV that handles black holes. The results show that the number of dropped packets decreased by up to ٤٨ percent, the throughput increased by up to ٨٠ percent and the packet delivery ratio increased by up to ٦٣ percent.

الملحق(أ)

المحاكي المستخدم

أ-١ تنصيب المحاكي المستخدم

لكي يتم تنصيب محاكي (GlomoSim) بشكل سليم يجب اتباع الخطوات التالية :

- نسخ مجلدي (GlomoSim) & (Parsec) إلى السواقة التي تحوي نظام التشغيل .
- تنصيب إصدار(٦,٠) من إصدارات لغة (Visual C++).

تنصيب JAVA JRE version ١,٢ or higher

JAVA SDK version ١,٢ or higher.

وذلك من اجل تنفيذ عملية المحاكاة عن طريق واجهة مرئية بنيت عن طريق لغة java.

- إضافة ما يلي :

c:\glomosim\bin;c:\parsec\bin;c:\glomosim;

إلى متحول (Path) الموجود في متحولات البيئة (Environment Variable) الموجودة بدورها في صفحة (Advanced) في أيقونة النظام (System) في لوحة التحكم (Control Panel) .

يتم بناء المحاكي عند كل تغيير في شفرة أحد ملفاته وفق التعليمة التالية:

C:\glomosim\main\makent

ويتم تنفيذه على ملف الإعداد وفق التعليمة التالية :

C:\glomosim\bin\glomosim config.in

أ-٢ وصف المحاكي المستخدم

يتألف المحاكي (GloMoSim) من عدة طبقات تستخدم كل منها بروتوكولاً خاصاً بهـــا وهـــي موضحة بالجدول المبين أدناه:

الجدول (أ-١) : طبقات المحاكي وبروتوكولاتها

Models	layer
TWO-RAY	Physical (Radio propagation)
٨٠٢,١١	Data link (Mac)
SNR-BOUNDED	Radio layer
AODV	Network (Routing)
TCP/IP	Transport
CBR (Constant Bit Rate)	Application

يحوي المحاكي (Glomosim) عدة ملفات أهمها ملف الإعداد (Config.in) والملف الذي يحـــوي سلسلة الإرساليات من المصادر إلى الأهداف (App.conf) والملف الذي يحوي النتائج النهائيـــة لعمل المحاكي (Glomo.state) .

أ-٢-١ ملف الإعداد (Config.in)

يحوي ملف الإعداد (Config.in) كل المعاملات التي سينفذ عليها السيناريو المقترح للشبكة اللاسلكية الآنية المتنقلة، ومن أهم هذه المعاملات وقت المحاكاة (Simulation Time)، يمثل هذا المعامل زمن تنفيذ المحاكي ولا يسمح بتجاوزه أثناء تحديد قيم زمن التوقف (Pause Time).

وبذرة المحاكاة (Seed) ويتحكم هذا المعامل بطريقة توزع العقد في الشبكة وعند كل تغيير لقيمته يتغير توزع العقد في الشبكة.

مقاييس الموقع (Terrain-Dimensions) يمثل هذا المعامل المساحة التي سيتم نشر العقد عليها

عدد العقد (Number-of-Nodes) يمثل هذا المعامل عدد العقد الموجودة أثناء المحاكاة.

الحركة (Mobility) يحدد هذا المعامل إمكانية وجود حركة في الشبكة، فإذا وجدت حركة فإن المعاملات التالية تحدد نمط الحركة:

نمط الحركة المستخدم (Mobility Random-Waypoint) يحدد هذا المعامل نمط الحركة العشوائية.

وقت التوقف (Mobility-Wp-Pause) يحدد هذا المعامل الزمن الذي تتوقف فيه العقدة عن الحركة.

أدنى سرعة للحركة (Mobility-Wp-Min-Speed) يحدد هذا المعامل السرعة الدنيا التي تتحرك فيها العقدة.

أقصى سرعة للحركة (Speed-Mobility-Wp-Max) يحدد هذا المعامل أقصى سرعة يمكن أن تتحرك فيها العقدة.

قوة الإرسال القصوى (Radio-Tx-Power) نستطيع من خلال تغيير قيمة هذا المعامل أن نتحكم بالمدى الراديوي للعقدة، ومن خلال التعليمة التالية نستطيع رؤية هذا المدى :

C:\glomosim\bin\radio_range config.in

أ-٢-٢ **ملف الإرساليات** (App.conf)

يحوي هذا الملف عدد الأزواج مصدر- وجهة، وحجم البيانات التي يتم إرسالها داخل الحزم والعدد ألأعظمي للحزم التي يستطيع مصدر إرسالها وعدد الحزم المرسلة خلال الثانية ووقت بداية الإرسال ونهايته وفي دراستي كان وقت الإرسال من بداية المحاكاة إلى نهايتها .

أ-٢-٣ **ملف النتائج** (Glomo.state)

يحوي هذا الملف نتائج المحاكاة النهائية ويمكن أن تكون هذه النتائج على مستوى طبقة التطبيق أو طبقة الشبكة أو أي طبقة أخرى وفق ما هو محدد في ملف الإعداد (config.in).

أ-٢-٤ ملف (Glomo.xls)

يحتوي هذا الملف المقاييس والإحصاءات المطلوبة للمقارنة بين البروتوكولات فقط وقد تم إنشاؤه بإجراء تعديلات بسيطة بربط شيفرة النتائج النهائية في البروتوكولات ببرنامج اكسل حيث يتم فتح ملف اكسل في نهاية كل عملية محاكاة ووضع النتائج فيه، وذلك لتسهيل إجراء العمليات الحسابية المطلوبة مثل إيجاد مجموع الإنتاجية للعقد، والعدد الكلى للحزم المحذوفة وغيرها.